A RISK-BASED AUDIT MODEL FOR INTERNAL AUDIT ENGAGEMENTS

A RISK-BASED AUDIT MODEL FOR INTERNAL AUDIT ENGAGEMENTS

by

Georgina Phillipina (Philna) Coetzee

THESIS

Submitted in fulfilment of the requirements for the degree

Philosophiae Doctor

in

AUDITING

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES
CENTRE FOR ACCOUNTING

at the

UNIVERSITY OF THE FREE STATE

under the supervision of

Professor D. S. Lubbe

November 2010

ABSTRACT

Many factors have played and are still playing contributing roles as to why internal auditors need to perform internal audit engagements more effectively and efficiently. The internal audit profession finds itself within a rapidly changing environment. The external factors affecting the profession include the various pieces of new guidance and legislation that are constantly being issued, the current global financial crisis, the occurrence of corporate and public scandals and the increased globalisation of the business environment, to name but a few. Internal factors within the organisation include management's increased demand for internal auditing to add value, the enhancement of coordination between all the various assurance providers, such as the external and internal auditors, and the increased role of internal auditing in assisting with the management of risks that threaten the achievement of the organisation's objectives. Within this environment the internal audit profession is growing at a tremendous rate, but at the same time it is reported that there is still a scarcity of competent internal auditors, especially in the fields of information technology and risk management. The Institute of Internal Auditors, as the governing body of the profession, is attempting to address this need by continuously issuing new professional guidance and performing research studies to provide its members with information and direction.

This study investigates the evolution of the internal audit profession as well as the concepts of corporate governance and risk management, and the role of internal auditing within these fields. It specifically focuses on how internal auditors can incorporate risk in the execution of an internal audit engagement to improve their methodology; thus performing engagements more effectively and efficiently. A comprehensive literature review was conducted on these topics and a preliminary risk-based internal audit engagement model was developed based on the literature. Thereafter, organisations in both the private and the public sectors in South Africa were examined via a maturity scorecard to determine which organisations were risk mature. The top five risk mature organisations in each sector were included in the second empirical study, with the main objective of obtaining input from their chief audit executives to refine the initial risk-based engagement model. Lastly, the model was tested in a practical scenario, using a case study approach, to determine whether there may be improvements in the execution of the internal audit engagement. The results of the three empirical studies were then used to finalise the model.

The study concludes that the risk-based internal audit model can be used during the planning phase of an assurance engagement, improving the process as follows:

- Areas with medium to high operational risks are included in the planning of the internal audit engagement.
- Low-risk areas are not included in the planning phase other than on a surprise basis according to the internal auditor's professional judgement.
- High-risk areas (inherent risk) that remain high after appropriate controls have been implemented (residual risk) are reported to management on a timely basis.

The use of this model will ensure that internal auditors focus on the areas that need urgent attention and not waste time on areas that are comparatively insignificant. This will mean that scarce internal audit resources can be allocated to areas where they will add the most value to the organisation. Although it was not a main objective of this study, it was found that the risk management framework and processes, and to a lesser extent the role of internal auditing regarding risk-related aspects within the public sector, need improvement to be in line with legislation, other guidance and best practices.

Keywords
Internal auditing, Corporate governance, Risk management, Risk-based internal auditing, Risk-based internal audit engagement model

Cut-off date for study purposes
With the concepts of corporate governance and risk management currently receiving much attention, new literature and guidance is published on a continuous basis. The cut-off date for the purpose of this study is set at 31 July 2010.

OPSOMMING

Verskeie faktore was en is tans nog relevante redes waarom interne ouditeure ‘n interne ouditaanstelling meer effektief en doeltreffend behoort uit te voer. Die interne ouditprofessie bevind homself tans in ‘n snel-veranderende omgewing. Eksterne faktore wat die professie beïnvloed is onder andere die konstante uitreiking van verskeie nuwe wetgewing en riglyne, die huidige wêreldwye finansiële krisis, korporatiewe en publieke skandale, en toenemende globalisasie in die besigheidsomgewing. Interne organisatoriese faktore sluit in bestuur se toenemende druk op interne ouditeure om waarde toe te voeg, toenemende koördinasie tussen die verskeie gerusstellingsfunksies, byvoorbeeld tussen die eksterne en interne ouditeure, en die toenemende rol van interne ouditering om bystand te verleen met die bestuur van risiko’s wat die bereiking van die organisasie se doelwitte mag belemmer. Binne hierdie omgewing is die interne ouditprofessie besig om teen ‘n geweldige koers te groei, maar terselfdertyd word daar gerapporteer dat daar ‘n skaarste aan bevoegde interne ouditeure is, veral in die velde van inligtingstegnologie en risikobestuur. Die Instituut vir Interne Ouditeure, die beheerliggaam van die professie, probeer om hierdie behoefte aan te spreek deur deurlopend nuwe professionele riglyne uit te reik en navorsing te onderneem om sodoende inligting en leiding aan hul lede te verskaf.

Hierdie studie ondersoek die ontwikkeling van die interne ouditprofessie asook die konsepte van korporatiewe bestuur en risikobestuur, en die rol wat interne oudit binne hierdie velde moet vertolk. Daar word spesifiek gefokus op hoe interne ouditeure risiko in die uitvoer van interne ouditaanstellings (‘audit engagements’) kan inkorporeer om sodoende hul metodologieë te verbeter; dus die meer effektiewe en doeltreffende uitvoer van aanstellings. ‘n Omvattende literatuurstudie oor hierdie onderwerpe is uitgevoer, en ‘n voorlopige risiko-gebaseerde interne oudit aanstellingsmodel, gebaseer op die literatuur, is ontwikkel. Organisasies in beide die privaat en publieke sektore is hierna aan die hand van ‘n bekwaamheidskeurkaart (‘risk maturity scorecard’) ondersoek, om te bepaal of die organisasie risiko bekwaam (‘risk mature’) is. Die top vyf risiko-bekwame organisasies in elke sektor is daarna in die tweede empiriese studie ingesluit, met die hoofdoelwit om die insette van die hoofde van interne ouditafdelings te verkry om sodoende die voorlopige risiko-gebaseerde aanstellingsmodel (‘engagement model’) te verfyn. Laastens is die model in ‘n praktiese situasie, deur middel van ‘n gevallestudiebenadering getoets, om te bepaal of daar moontlike verbeterings in die uitvoer van die

interne ouditaanstelling is. Die resultate van die drie empiriese studies is daarna gebruik om die model te finaliseer.

Die gevolgtrekking van die studie is dat die risiko-gebaseerde interne ouditmodel gebruik kan word tydens die beplanningsfase van ‘n gerusstellingsaanstelling ten einde die proses soos volg te verbeter:

- Areas met medium tot hoë operasionele risiko’s word ingesluit in die beplanning van die interne ouditaanstelling.
- Lae risiko areas word nie in die beplanningsfase ingesluit nie, behalwe op ‘n verrassingsgrondslag, gebaseer op die interne ouditeur se professionele oordeel.
- Hoë risiko areas (inherente risiko) wat, nadat toepaslike kontroles ingestel is, hoog bly (reswaarde risiko – ‘residual risk’), moet aan bestuur op ‘n tydige basis gerapporteer word.

Die gebruik van hierdie model kan verseker dat interne ouditeure op die areas wat dringend aandag benodig fokus, en nie tyd sal vermors op areas wat vergelykenderwys irrelevant is nie. Dit kan beteken dat skaars interne oudit-hulpbronne geallokeer kan word na areas waar dit die meeste waarde tot die organisasie kan toevoeg. Alhoewel dit nie ‘n hoofdoelwit van hierdie studie was nie, is daar bevind dat die risiko bestuurraamwerk en -prosesse, en tot ‘n mindere mate die rol van die interne ouditeur aangaande risiko-relevante aangeleenthede, in die publieke sektor verbeter moet word om met wetgewing, ander riglyne en beste-praktyke in lyn gebring te word.

ACKNOWLEDGEMENTS

I wish to acknowledge the support, encouragement and contribution made to this study by family, friends, colleagues and practitioners. As most of these individuals are Afrikaans-speaking, this will be done in Afrikaans and, where applicable, in English.

Eerstens wil ek baie dankie sê aan Prof Dave Lubbe. Ek het nie net baie oor die vakgebied geleer nie, maar ook oor wat nodig is om ‘n studie van hierdie omvang aan te pak en deur te voer. Dankie dat u altyd daar was vir raad en leiding, u vinnige terugvoer en bemoedigende woorde. Mag ek die beginsels wat u my geleer het toepas indien ek eendag iemand moet lei.

Dankie aan my kollegas by die Universiteit van Pretoria, veral diè wat vir my verantwoordelikhede ingestaan het. Ek dink spesifiek aan Rudrik du Bruyn, Ane Kritzinger en Vanessa White. Dankie ook aan die ander vir jul ondersteuning en bemoedigende woorde.

Daar was verskeie mense wat tot ‘n mindere of meerdere mate raad en insette gelewer het. Ek dink veral aan Prof Karin Barac, Prof Herman de Jager, Kato Plant, Houdini Fourie, Rina Owen, John du Plessis, Moray Smit, Jan Lubbe, Sean de la Rosa en die hoofde van interne ouditafdelings wat bereid was om my in hul besige skedules te akkommodeer.

Thank you Farida Omar for typing some of the more difficult figures and Pam Apps for the professional editing of this comprehensive document.

Om saam met ‘n persoon wat so ‘n studie onderneem onder een dak te woon is ‘n moeilike taak. Baie dankie aan my man Stephan en kinders Jana en Ansu dat hulle my ‘ek is besig’ tye verdra het. Ook aan my vriendin Esther vir haar ondersteuning en bemoediging, asook my selgroep-vriende vir al die gebede.

Hierdie studie word opgedra aan my Koning, Jesus Christus, wat my die vermoë gegee het om hierdie taak te voltooi, en my deurentyd gedra het.

TABLE OF CONTENTS

ABSTRACT iii

OPSOMMING v

ACKNOWLEDGEMENTS vii

INDEX viii

LIST OF TABLES xx

LIST OF FIGURES xxiii

ABBREVIATIONS xxiv

TERMINOLOGIES xxvi

INDEX

CHAPTER 1

INTRODUCTION TO THE STUDY AND RESEARCH METHODOLOGY 1

1.1 INTRODUCTION 1

1.2 THE CHANGING INTERNAL AUDIT ENVIRONMENT 4

1.2.1 Brief background to the structure and globalisation of the internal audit profession 5

1.2.2 Growth within the profession 6

1.2.3 Scarcity of competent internal auditors 8

1.2.4 Guidance issued by the Institute of Internal Auditors 9

1.2.4.1 International Professional Practices Framework (IIA Inc.) 9

1.2.4.2 Common body of knowledge (IIA Inc.) 9

1.2.4.3 Competency framework (IIA Inc.) 10

1.2.4.4 Institute of Internal Auditors position paper: Organisational governance – guidance for internal auditors (IIA Inc. and IIA (Australia)) 10

1.2.4.5 Institute of Internal Auditors position paper: The role of internal auditing in enterprise-wide risk management issues (IIA (UK and Ireland)) 11

1.2.4.6 Institute of Internal Auditors position paper: Risk-based internal auditing (IIA (UK and Ireland)) 11

1.2.4.7	Application of the guidance	11
1.2.5	Conclusion	12
1.3	CORPORATE GOVERNANCE	12
1.3.1	Corporate governance codes	13
1.3.2	Corporate governance legislation	14
1.3.2.1	South African legislation on corporate governance	15
1.3.2.2	United States of America legislation on corporate governance	16
1.3.3	Corporate governance in other countries	16
1.3.4	Corporate scandals	17
1.3.5	Conclusion	19
1.4	EXTERNAL AUDITORS	20
1.4.1	Guidance on the external auditors' use of the work of the internal auditor	20
1.4.2	The external auditors' use of the work of the internal auditor	21
1.4.3	External auditing for the public sector	21
1.4.4	Conclusion	22
1.5	INTERNAL AUDITING IN THE PRIVATE AND THE PUBLIC SECTORS	24
1.5.1	Differences	24
1.5.2	Similarities	27
1.5.3	Legislation and other regulations	28
1.5.4	Conclusion	29
1.6	CHANGES IN INTERNAL AUDIT METHODOLOGY	29
1.6.1	Need for change	29
1.6.2	Change in the way internal audit engagements are performed	30
1.6.3	Conclusion	32
1.7	RISK-BASED INTERNAL AUDITING	32
1.7.1	Definition of risk	32
1.7.2	Risk management as a cornerstone of corporate governance	33
1.7.3	Internal auditing and the concept of risk	34
1.7.3.1	Risk management	35

1.7.3.2	Planning the internal audit function's activities based on risk	35
1.7.3.3	Risk-based internal audit engagements	35
1.7.4	Important sources on risk-based internal auditing	35
1.7.4.1	Institute of Internal Auditors Incorporated	36
1.7.4.2	Brief overview on literature	37
1.7.5	Conclusion	38
1.8	PROBLEM STATEMENT AND RESEARCH METHODOLOGY	39
1.8.1	Research problem	39
1.8.2	Research objective	40
1.8.3	Scope and limitations	41
1.8.4	Research methodology	42
1.8.4.1	Literature review	42
1.8.4.2	Empirical studies	44
1.8.4.2.1	Risk maturity	44
1.8.4.2.2	Risk-based internal audit model	48
1.8.4.2.3	Test the model (case study)	51
1.8.5	Conclusion	52
1.9	LAYOUT OF THE STUDY	53
1.10	CONCLUSION	54

CHAPTER 2

THE EVOLUTION OF THE INTERNAL AUDIT PROFESSION 57

2.1	INTRODUCTION	57
2.2	THE HISTORY OF AUDITING AND INTERNAL AUDITING	58
2.2.1	The history from a global perspective	58
2.2.2	The evolving role of the Institute of Internal Auditors	60
2.2.3	Developments in South Africa	61
2.2.4	Conclusion	63
2.3	THEORY OF INTERNAL AUDITING	63
2.3.1	Comparison of internal and external auditing	64
2.3.2	External auditing and the agency and accountability theories	67
2.3.3	Internal auditing and the agency and accountability theories	68

2.3.4	Conclusion	70
2.4	CHANGES WITHIN THE INTERNAL AUDIT PROFESSION	70
2.4.1	Definition of internal auditing	70
2.4.1.1	Consulting activity	71
2.4.1.2	Adding value	73
2.4.1.3	Corporate governance and risk management	73
2.4.1.4	Necessity of the changes in the definition	74
2.4.2	In-house, outsourcing and co-sourcing	75
2.4.3	Specialisation fields	79
2.4.4	Professional guidance	81
2.4.4.1	International professional practices framework	81
2.4.4.2	Other Institute of Internal Auditors guidance	83
2.4.5	Conclusion	84
2.5	EXTERNAL FACTORS AFFECTING THE INTERNAL AUDIT PROFESSION	84
2.5.1	Globalisation	84
2.5.2	Corporate governance and internal auditing	87
2.5.2.1	Corporate governance codes	90
2.5.2.2	Other corporate governance-related guidance and legislation	92
2.5.2.3	Corporate governance in South Africa	96
2.5.2.3.1	Private sector	101
2.5.2.3.2	Public sector	102
2.5.2.4	Corporate scandals affecting internal auditing	103
2.5.2.4.1	Some major global corporate scandals	104
2.5.2.4.2	Some South African corporate scandals	105
2.5.3	Recognition of internal auditing by role players	106
2.5.3.1	Parties within the organisation	107
2.5.3.1.1	Board of directors and its committees	107
2.5.3.1.2	Senior management	108
2.5.3.2	Parties from outside the organisation	109
2.5.3.2.1	Shareholders	109
2.5.3.2.2	External auditors	110
2.5.4	Conclusion	112

2.6	THREATS TO THE INTERNAL AUDIT PROFESSION	113
2.6.1	Independence	113
2.6.2	Corporate governance requirements	117
2.6.3	Scarcity of competent and skilled internal auditors	119
2.6.4	The scope of internal audit activities	122
2.6.5	Global financial crisis	123
2.6.6	Technology	126
2.6.7	Conclusion	130
2.7	EFFECTIVE AND EFFICIENT INTERNAL AUDIT FUNCTION	130
2.8	SUMMARY AND RELEVANCE TO THE STUDY	133

CHAPTER 3
THE DEVELOPMENT OF CORPORATE GOVERNANCE WITH SPECIFIC REFERENCE TO RISK MANAGEMENT **137**

3.1	INTRODUCTION	137
3.2	CORPORATE GOVERNANCE	138
3.2.1	Introduction to corporate governance	139
3.2.2	The definition of corporate governance	141
3.2.3	Factors influencing the need for and value of new developments	145
3.2.3.1	Corporate scandals	146
3.2.3.2	Investors' requirements	147
3.2.3.3	Principle-driven (codes) *versus* rule-driven (legislation) guidance	149
3.2.4	Accountability as an element of corporate governance	150
3.2.5	Conclusion	152
3.3	RISK MANAGEMENT AS PART OF CORPORATE GOVERNANCE	153
3.3.1	Introduction to risk management	153
3.3.2	The definition of risk management	155
3.3.3	Motivation for effective risk management	160

3.3.4	Corporate governance guidelines and regulations influencing risk management	163
3.3.4.1	Global guidelines	163
3.3.4.2	South African guidelines and legislation	165
3.3.4.2.1	Private sector	170
3.3.4.2.2	Public sector	171
3.3.5	Risk management standards	173
3.3.5.1	Private sector	173
3.3.5.2	Public sector	175
3.3.6	Responsibilities of various parties	177
3.3.6.1	Board of directors and risk committee	177
3.3.6.2	Senior management and chief risk officer/risk department	179
3.3.6.3	Internal auditing	181
3.3.7	Conclusion	181
3.4	THE CONCEPT OF RISK AS REFLECTED IN RISK MANAGEMENT	182
3.4.1	Generic definition of risk	182
3.4.2	Risk in the business environment	184
3.4.3	Business risk as part of corporate governance's risk management	187
3.4.3.1	Uncertainty relating to business risk	188
3.4.3.2	Loss as a result of threats (hazards)	188
3.4.3.3	Loss of opportunities	189
3.4.4	Types of risks related to risk management	189
3.4.4.1	Inherent risk	190
3.4.4.2	Residual risk	190
3.4.5	Conclusion	191
3.5	RISK MANAGEMENT PROCESS	191
3.5.1	Comparison of different models for a risk management process	192
3.5.2	Elements within the risk management process	195
3.5.2.1	Objective setting	195
3.5.2.2	Identification of risk	196

3.5.2.3	Assessment of risks identified	198
3.5.2.3.1	Risk appetite	200
3.5.2.3.2	Risk tolerance	200
3.5.2.4	Risk responses	201
3.5.2.5	Risk communication	202
3.5.2.6	Risk monitoring	202
3.5.3	Risk register	203
3.5.4	Conclusion	204
3.6	RISK MATURITY	205
3.6.1	Introduction	205
3.6.2	Risk maturity model	207
3.6.2.1	Comparison of different models	208
3.6.2.2	Common criteria used	211
3.6.3	Conclusion	213
3.7	FUTURE OF RISK MANAGEMENT	214
3.7.1	Possible weaknesses in the implementation and application of risk management	214
3.7.1.1	Lack of commitment	216
3.7.1.2	Risk management (silo approach) *versus* enterprise risk management (holistic approach) resulting in neglecting strategic and/or operational risks	217
3.7.2	Current trends and new developments	219
3.7.3	Conclusion	221
3.8	SUMMARY AND RELEVANCE TO THE STUDY	222

CHAPTER 4

THE ROLE OF INTERNAL AUDITING WITH SPECIFIC REFERENCE TO RISK **227**

4.1	INTRODUCTION	227
4.2	CORPORATE GOVERNANCE AND INTERNAL AUDITING	228
4.2.1	Guidance on corporate governance by the Institute of Internal Auditors	228

4.2.1.1	International Professional Practices Framework – *Standards* and practice advisories	228
4.2.1.2	International Professional Practices Framework – Organisational governance: guidance for internal auditors	229
4.2.2	Roles and responsibilities	229
4.2.3	Conclusion	232
4.3	RISK AND INTERNAL AUDITING	232
4.3.1	Risk management	234
4.3.1.1	Guidance on risk management	234
4.3.1.1.1	Guidance by the Institute of Internal Auditors Incorporated	235
4.3.1.1.2	South African guidance	238
4.3.1.2	Influencing factors	239
4.3.1.3	Conclusion	241
4.3.2	Annual planning of the internal audit function's activities	242
4.3.2.1	Guidance on internal audit annual planning	243
4.3.2.1.1	Guidance by the Institute of Internal Auditors Incorporated	243
4.3.2.1.2	South African guidance	244
4.3.2.2	Influencing factors	244
4.3.2.3	Conclusion	246
4.3.3	Internal audit engagements	246
4.3.3.1	Guidance on internal audit engagements	247
4.3.3.1.1	Guidance by the Institute of Internal Auditors Incorporated	248
4.3.3.1.2	Guidance by the Institute of Internal Auditors (UK and Ireland)	248
4.3.3.1.3	South African guidance	249
4.3.3.2	Influencing factors	249
4.3.3.3	Conclusion	250
4.4	INTERNAL AUDIT ASSURANCE ENGAGEMENTS	251
4.4.1	Internal audit process	251
4.4.2	Planning phase	253
4.4.3	Engagement work programme	257
4.4.4	Conclusion	258
4.5	RISK-BASED INTERNAL AUDIT ENGAGEMENT	258

4.5.1	Introduction to risk-based internal audit engagement	259
4.5.2	The definition of a risk-based internal audit engagements	261
4.5.3	Elements needed to perform a risk-based internal audit engagement	264
4.5.3.1	Risk maturity	264
4.5.3.2	Risk register	266
4.5.3.3	Operational risk assessment	267
4.5.4	Risk-based internal audit engagement models	268
4.5.4.1	Basis of risk-based internal audit models	268
4.5.4.2	Comparison of different internal audit methodologies	270
4.5.5	Preliminary risk-based internal audit engagement model	274
4.5.6	Conclusion	282
4.6	FUTURE OF INTERNAL AUDITING'S ROLE IN RISK	283
4.6.1	Problems experienced by internal auditing	284
4.6.1.1	Qualitative and quantitative risk assessment	285
4.6.1.2	Risk related knowledge of internal auditors	286
4.6.2	Current trends and new developments	288
4.6.3	Expectations of role players	289
4.6.3.1	Management's expectations	290
4.6.3.2	Internal auditing's expectations	292
4.6.4	Conclusion	294
4.7	SUMMARY AND RELEVANCE TO THE STUDY	295

CHAPTER 5

RESEARCH RESULTS OF THE EMPIRICAL STUDIES: RISK MATURITY,REFINING THE RISK-BASED INTERNAL AUDIT ENGAGAMENT MODEL AND TESTING THE MODEL **300**

5.1	INTRODUCTION	300
5.2	STATUS OF RISK WITHIN SOUTH AFRICAN ORGANISATIONS	301
5.2.1	Use of risk maturity model	301
5.2.1.1	The Risk and Insurance Management Society Incorporation model	302

5.2.1.2	Adopt for South African corporate governance requirements	302
5.2.1.3	Final risk maturity scorecard	303
5.2.2	Empirical study's scope and limitations	303
5.2.3	Risk maturity score	304
5.2.4	Conclusion	306
5.3	OBTAIN INPUT INTO THE RISK-BASED INTERNAL AUDIT MODEL	306
5.3.1	The development of a structured interview schedule	307
5.3.1.1	The relevance and importance of risk management for the organisation and the internal audit function	307
5.3.1.2	Determine whether the internal audit function includes risk concepts in its activities	311
5.3.1.3	Determine whether the internal audit function incorporates risk-based planning in their internal audit engagements	312
5.3.1.4	Obtain input into the preliminary developed risk-based internal audit engagement model and adapt the model accordingly	312
5.3.2	Refine the questionnaires	313
5.3.3	Empirical study's scope and limitation	313
5.3.4	Discussion of results	315
5.3.4.1	The relevance and importance of risk management for the organisation and the internal audit function	316
5.3.4.1.1	Factors influencing the standing of the internal audit function	316
5.3.4.1.2	Existence and structures of various risk-related parties	323
5.3.4.1.3	Coordination of risk-related activities	327
5.3.4.1.4	Adherence to the IIA *Standards*	331
5.3.4.1.5	Internal auditing's involvement in risk management	336
5.3.4.1.6	Internal audit activities related to the risk management framework	341
5.3.4.1.7	Internal audit activities related to the risk management process	344
5.3.4.2	Inclusion of risk concepts into the internal audit function's activities	348

5.3.4.3	Risk-based planning of internal audit engagements	351
5.3.4.4	Risk-based internal audit model	355
5.3.5	Conclusion	358
5.4	TEST THE MODEL (CASE STUDY)	359
5.4.1	Criteria for test sample(s)	359
5.4.2	Additional required criteria and information	360
5.4.3	Criteria for choosing an audit engagement	361
5.4.4	Structure of the case study	362
5.4.5	Case study's scope and limitation	363
5.4.6	Result of the case study	364
5.4.6.1	Problems encountered during execution	364
5.4.6.2	Discussion of results	365
5.4.7	Conclusion	366
5.5	REFINE THE MODEL	368
5.6	CONCLUSION	373

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS		**375**
6.1	INTRODUCTION	375
6.2	NEED FOR CHANGE IN THE WAY INTERNAL AUDIT ENGAGEMENT ARE PERFORMED	375
6.3	THE EVOLUTION OF INTERNAL AUDITING	376
6.4	RISK MANAGEMENT AS PART OF CORPORATE GOVERNANCE	379
6.5	THE ROLE OF INTERNAL AUDITING WITH REGARD TO RISK	384
6.6	RECOMMENDATIONS	390
6.6.1	The board and management	391
6.6.1.1	All organisations	391
6.6.1.2	Private sector organisations	391
6.6.1.3	Public sector organisations	392
6.6.2	Risk management structures	392
6.6.2.1	All organisations	392

6.6.2.2	Private sector organisations	393
6.6.2.3	Public sector organisations	393
6.6.3	Chief audit executives	393
6.6.3.1	All organisations	393
6.6.3.2	Private sector organisations	394
6.6.3.3	Public sector organisations	394
6.6.4	Internal auditors	394
6.6.5	Institute of Internal Auditors	395
6.7	FUTURE RESEARCH	395
6.8	RESEARCH CONCLUSION	396
6.9	FINAL CONCLUSION	397

LIST OF REFERENCES 399

Annexure A	National and international theses and dissertations related to the study (2000 to current)	451
Annexure B	Summary of Risk & Insurance Management Society (RIMS) risk maturity model steps	459
Annexure C	Maturity model criteria	460
Annexure D	Deliverables matrix	463
Annexure E	Risk maturity attributes and levels	466
Annexure F	Risk maturity model score card	474
Annexure G	Private sector: top 40 companies listed on the JSE Limited as per market capital on 08/04/2009	477
Annexure H	Public sector - national government organisations as on 18/06/2009	479
Annexure I	Structured interview schedule: private sector	481
Annexure J	Structured interview schedule: public sector	491

LIST OF TABLES

1.1	Summary of membership and certified internal auditors globally and in South Africa	7
1.2	Audit reports for the provincial government for the 2007/2008 financial year	23
2.1	Comparison between internal auditing and external auditing (financial statement audit) in a South African context	66
2.2	Comparison of the previous and current definitions of internal auditing	71
2.3	Inclusion of internal auditing in global corporate governance guidance	89
2.4	Evolution of corporate governance codes and related documents with regard to internal auditing	91
2.5	Evolution of internal auditing with reference to South African corporate governance codes	99
2.6	Technology affecting the internal audit profession	128
3.1	Inclusion of risk management in global corporate governance and other guidance	164
3.2	Evolution of risk management in South African corporate governance codes	166
3.3	Three elements of risk within risk management	187
3.4	Comparison of various risk management process models	193
3.5	Risk maturity models	209
4.1	The IIA internal audit engagement planning linked to the risk management process	256
4.2	Evolution of the internal audit engagement	260
4.3	The effect of risk maturity on a risk-based internal audit engagement	265
4.4	Comparing evolution of internal audit engagements with the COSO models	269
4.5	COSO I and COSO II used in practice as part of the internal audit engagement planning process	272

4.6	Incorporating the risk management process into the internal audit engagement process	275
5.1	Analysis of data on risk maturity	305
5.2	Risk maturity score agreement	316
5.3	Structure and type of activities of the internal audit function	317
5.4	Number of staff	319
5.5	Competencies of internal auditors	320
5.6	Internal audit function's budget	322
5.7	Reporting lines of the chief audit executive	323
5.8	Existence of an audit and/or risk committee and other risk structures	324
5.9	Composition of the audit and/or risk committees	325
5.10	Reporting lines of risk structures	327
5.11	Coordination between the internal audit function and the internal risk structures	328
5.12	Coordination between the audit committee and the risk committee	329
5.13	Coordination between the internal audit function and the risk committee/audit and risk committee	330
5.14	Adherence to standards related to risk management activities	332
5.15	Adherence to standards related to planning the internal audit function's annual activities	334
5.16	Adherence to standards related to the performance of risk-based internal auditing engagements	335
5.17	Viewpoint on the areas of involvement in risk management	336
5.18	Viewpoint on the increased involvement in risk management	337
5.19	Viewpoint on the future increased involvement in risk management	338
5.20	Factors influencing the public sector's involvement in risk management	340
5.21	Current and future activities related to the risk management framework (consulting *versus* assurance activities)	342

5.22	Factors hindering the public sector's involvement in the risk management framework	343
5.23	The level of implementing a risk management process(es) and the implementation of a risk register	344
5.24	Parties responsible for the risk management process(es) on various organisational levels	345
5.25	Update of the risk register	346
5.26	The role of internal auditing in the risk management process	347
5.27	Adherence to guidance related to the risk-based planning of the internal audit function's annual plan	349
5.28	Factors hindering public sector internal auditing from adhering to guidance on planning the function's annual plan	350
5.29	Methodology used during internal audit engagements	352
5.30	The elements in use as the starting point of the planning phase	352
5.31	The information obtained on key elements of the risk-based internal audit engagement planning phase	353
5.32	Underdeveloped areas in a risk-based internal audit engagement	355
5.33	Viewpoints of the use and benefits of a risk-based internal audit engagement model	356
5.34	Treatment when the inherent risk is low	357
5.35	Treatment when the movement of inherent to residual risk is unsatisfactory	358
5.36	Problems encountered during the testing of the model	365
5.37	Summary of results of the case study	367
5.38	Comparing the preliminary model, input received form CAEs and the results of the case study	369

LIST OF FIGURES

2.1	Internal auditing and the agency and accountability theories	69
2.2	Various dimensions of modern internal auditing	74
4.1	IIA position statement on internal auditings' role in Enterprise Risk Management	237
4.2	The risk management process and internal audit engagement planning	257
4.3	Mitigation of risks according to the risk management process	277
4.4	Risk-based internal audit engagement based on the risk management process	279

ABBREVIATIONS

AGSA	Auditor General South Africa
AIRMIC	Association of Insurance and Risk Managers
ANC	African National Congress
AS/NZS	Australian Standards Board / New Zealand Standards Board
ASX	Australian Securities Exchange
CAATTs	Computer Assisted Audit Tools and Techniques
CACG	Commonwealth Association for Corporate Governance
CAE	Chief Audit Executive
CA(SA)	Chartered Accountant (South Africa)
CBOK	Common Body of Knowledge
CEO	Chief Executive Officer
CFIA	Competency Framework for Internal Auditors
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CoCo	Criteria of Control (Board)
COO	Chief Operating Officer
COSO	Committee of Sponsoring Organisations
CRO	Chief Risk Officer
ECGI	European Corporate Governance Institute
ECIIA	European Confederation of Institutes of Internal Auditing
ERM	Enterprise Risk Management
FRC	Financial Reporting Council
GAIN	Global Audit Information Network
IACCM	International Association for Contract & Commercial Management
IAF	Internal Audit Function
IFAC	International Federation of Accountants
IIA	Institute of Internal Auditors
IIA Inc.	Institute of Internal Auditors Incorporated
iKUTU	Institute of Internal Auditors (South Africa), KPMG, University of Pretoria, Tshwane University of Technology & University of South Africa
IOD	Institute of Directors

IPPF	International Professional Practices Framework
IRM	Institute of Risk management
ISO	International Organisation for Standardisation
IT	Information Technology
JSE	Johannesburg Stock Exchange
MFMA	*Municipal Finance Management Act, No 56 of 2003*
MIT	Massachusetts Institute of Technology
N.d.	Not dated
NDLTD	Networked Digital Library of Theses and Dissertations
NRF	National Research Foundation
NYSE	New York Stock Exchange
OECD	Organisation for Economic Co-operation and Development
PFMA	*Public Finance Management Act, No 1 of 1999*
PPF	Professional Practices Framework
PRMIA	Professional Risk Managers' International Association
PWC	PricewaterhouseCoopers
RIMS	Risk and Insurance Management Society Incorporated
SA	South Africa
SAICA	South African Institute of Chartered Accountants
SAPA	South African Press Association
SEI	Software Engineering Institute
SOX	*Sarbanes Oxley Act, 2002*
Standards	International Standards for the Professional Practice of Internal Auditing
UK	United Kingdom
UMI	University Microfilm International
USA	United States of America

TERMINOLOGIES

Terminology	Definition	Source(s)
Assurance services	*An objective examination of evidence for the purpose of providing an independent assessment of governance, risk management, and control processes for the organisation. Examples may include financial, performance, compliance, system security, and due diligence engagements.*	IIA 2009(a):40
Audit universe	*A compilation of the subsidiaries, business units, departments, groups, processes, or other established subdivisions of an organisation that exist to manage one or more business risks.*	Reding *et al.* 2009:4-19
Chief audit executive	*Chief audit executive is a senior position within the organisation responsible for internal audit activities. Normally, this would be the internal auditor director. In the case where internal audit activities are obtained from external service providers, the chief audit executive is the person responsible for overseeing the service contract and the overall quality assurance of these activities, reporting to senior management and the board regarding internal audit activities, and the follow-up of engagement results. The term includes titles such as general auditor, head of internal audit, chief internal auditor and inspector general.*	IIA 2009(a):40
Consulting services	*Advisory and related client service activities, the nature and scope of which are agreed with the client, intended to add value and improve an organisation's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation and training.*	IIA 2009(a):40

Terminology	Definition	Source(s)
Effective	*Producing a desired or intended result.*	Oxford Dictionary 2005:370
Efficient	*Working productively with minimum wasted effort and expense.*	Oxford Dictionary 2005:370
Engagement procedures	*Specific tasks performed by the internal auditor to gather the evidence required to achieve the prescribed audit objectives.*	Reding *et al*. 2009:10-4
Engagement work programme	*A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.*	IIA 2009(a):41
Enterprise risk management (ERM)	*Enterprise risk management is defined as comprehensive risk management that allows companies to identify, prioritise, and effectively manage their crucial risks. An ERM approach integrates risk solutions into all aspects of business practices and decision making processes.*	IOD 2009:118 Refer to section 3.5 on p. 191
Governance	*The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organisation toward the achievement of its objectives.*	IIA 2009(a):41 Refer to section 3.2.2 on p. 141
Impact	*The result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the entity's related objectives.*	COSO 2004:122
Inherent risk	*The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.*	COSO 2004:122

Terminology	Definition	Source(s)
Internal audit engagement	*A specific internal audit engagement or project that includes multiple tasks or activities designed to accomplish a specific set of objectives – also refer to assurance services and consulting services.* *A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.*	Reding *et al.* 2009:1-6 IIA 2009(a):40
Internal audit function	*A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organisation's operations. The internal audit activity helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.*	IIA 2009(a):41
Internal audit process	*… internal assurance and consulting engagements must be performed in a systematic and disciplined manner…:* • *planning…;* • *performing…;* • *communicating engagement outcomes.*	Reding *et al.* 2009:1-6
Likelihood	*The possibility that a given event will occur. Terms sometimes take on more specific connotations, with 'likelihood' indicating the possibility that a given event will occur in*	COSO 2004:123

Terminology	Definition	Source(s)
	qualitative terms such as high, medium, and low, or other judgmental scales and 'probability' indicating a quantitative measure such as a percentage, frequency of occurrence, or other numerical metric.	
Operational activities, objectives and risks	*These pertain to the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.* *Operations objectives related to the effectiveness and efficiency of the entity's operations. They include related sub-objectives for operations, directed at enhancing operating effectiveness and efficiency in moving the enterprise toward its ultimate goal.* *Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.*	COSO 2004:36 COSO 2004:37 Basle Committee 2004
Organisation	*An organisation of any size established for a particular purpose…. for example, may be a business enterprise, not-for-profit organisation, government body, or academic institution. Terms used as synonyms include entity and enterprise.*	COSO 2004:122
Private sector	*The term Private sector organisations includes all organisations that are privately owned, including public-owned companies, private-owned companies, closed corporations, partnerships and sole proprietaries.*	Refer to section 1.5 on p. 24

Terminology	Definition	Source(s)
Public sector	*Public sector organisations include all organisations that are governed or partially governed by the government.*	Refer to section 1.5 on p. 24
Residual risk	*The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.*	IIA 2009(a):41
Risk appetite	*The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision).* *The level of residual risk that the company is prepared or willing to accept without further mitigation action being put in place, or the amount of risk the company is willing to accept in pursuit of value. A company's risk appetite will vary....*	COSO 2004:124 IOD 2009:125
Risk assessment	*Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.* *Overall process of risk identification, risk quantification and risk evaluation in order to identify potential opportunities or minimise loss.*	COSO 2004:6 IOD 2009:125
Risk indicator /Risk factor	*A metric that can be monitored and that has a correlation with one of the risk factors (indicators by which key risks can be easily identified).*	IOD 2009:124
Risk management	Comprehensive for *risk management framework* and *risk management process*.	
Risk management framework	*…entails the planning, arranging and controlling of activities and resources to minimise the negative impacts of all risks to levels that can be*	IOD 2009:123 Refer to section 3.3.1

Terminology	Definition	Source(s)
	tolerated by stakeholders whom the board has identified as relevant to the business of the company, as well as to optimise the opportunities, or positive impacts, of all risks.	on p. 153
Risk management process	*… is the identification and evaluation of actual and potential risk areas as they pertain to the company as a total entity, followed by a process of either avoidance, termination, transfer, tolerance (acceptance), exploitation, or mitigation (treatment) of each risk, or a response that is a combination of integration.* *A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives.*	IOD 2009:123 Refer to section 3.3.1 on p. 53 IIA 2009(a):41
Risk maturity	*The extent to which a robust risk management approach has been adopted and applied, as planned, by management across the organisation to identify, assess, decide on responses to and report on opportunities and threats that affect the achievement of the organisation's objectives.* *When the risk management philosophy is well developed, understood and embraced by its personnel….*	De la Rosa 2008(b) COSO 2004:28
Risk register	*A formal listing of risks identified, together with the results of the risk analysis, risk evaluation procedures together with details of risk treatment, risk control, risk reduction plans.*	IOD 2009:126
Risk response	*Management selects risk responses – avoiding, accepting, reducing or sharing risk – developing a*	COSO 2004:6

Terminology	Definition	Source(s)
	set of actions to align risks with the entity's risk tolerances and risk appetite.	
Risk tolerance	*The acceptable variation relative to the achievement of an objective.*	COSO 2004:124
Risk-based internal auditing	*Risk-based internal auditing (RBIA) is the methodology [that] provides assurance that risks are being managed to within the organisation's risk appetite.*	Griffiths 2006(b):1
Significant findings	*The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.*	IIA 2009(a):41
Strategic activity, objectives and risks	*Strategic objectives are high-level goals, aligned with and supporting the entity's mission/vision. Strategic objectives reflect management's choice as to how the entity will seek to create value for its stakeholders.* *…management identifies risks associated with a range of strategy choices….*	COSO 2004:35
Target risk	Refer to *risk tolerance* and *risk appetite.*	
Traditional auditing	*…profession developed…type of audit services…:* • *internal check procedures;* • *transaction-based approach;* • *probity-based work;* • *risk analysis;* • *system-based approach;* • *operational audit;* • *management audit…*	Spencer Pickett 2003:10-12

CHAPTER 1
INTRODUCTION TO THE STUDY AND RESEARCH METHODOLOGY

1.1 INTRODUCTION

The challenges of today's changing world introduce great opportunities for governments and businesses, and their respective managements. The increasing demand for accountability as a result of corporate scandals, the complexity of the business environment, natural disasters that have had an influence on the business environment, globalisation, the scarcity of skills, and many more, places the spotlight on sound corporate governance principles – for both the private and the public sectors. The business environment is finding itself in extraordinarily difficult financial circumstances as a result of the current global financial crisis (Keen 2008). At the 2009 World Economic Forum it was reported that this global financial crisis has destroyed between 40% and 45% of the world's wealth, affecting every country, industry, organisation and individual (Lam 2009:22). Worldwide people are losing their jobs, organisations are closing their doors, and well-known organisations went bankrupt. Many argue that the core of this crisis is the lack of an effective and efficient risk management framework (Lam 2009:23; Hull 2009:3).

It is time for the business environment to turn back to the basic principles of sound management strategies. Worldwide, government institutions and private sector companies (hereafter all referred to as organisations) have issued corporate governance codes and legislation to provide guidance on these concepts. Two of the elements incorporated into most of these codes and legislation are risk management and internal auditing. In South Africa (SA), with the issuing of the three King reports (IOD 1994, 2002, 2009), the growing importance of both internal auditing as well as risk management, as cornerstones of corporate governance, is demonstrated.

Open Rubric

The internal audit function is viewed by many global leaders as being in an ideal situation to assist management with business aspects such as improving governance, the evaluation of operational effectiveness, the addressing of risks threatening the organisation achieving its objectives, and generally adding value to the organisation (Bou-Raad 2000:186; Baker & Owsen 2002:785; Nagy & Cenker 2002:131; Ramamoorti 2003:9; Hermanson & Rittenberg 2003:32; Rittenberg, Johnson, Krogstad, Richards, Roth, McPhilimy cited in Chapman 2004:42-47; Campbell, Adams, Campbell & Rose 2006:44; Krell 2006:36; PWC 2008(a):3; IOD 2009:93). Especially in these times of increasingly and rapid change and the current global financial crisis, internal auditing could be crucial to ensuring efficient operations, effective controls and risk management strategies, all contributing to strong corporate governance (Arena, Arnaboldi & Azzone 2006:288; Goodwin-Stewart & Kent 2006(b):95; Chambers cited in McCollum 2009:47). This statement is supported by the fact that two of the most well-known corporate scandals that influenced the United States of America's (USA) financial world, namely Enron and WorldCom, were linked to internal auditing, with the wrongdoings at WorldCom being discovered and made public by the internal auditors (Markham 2006:344). Roger W. Raber (cited in Jackson 2005(a):70), President of the National Association of Corporate Directors in the USA, states:

> I cannot think of a time when internal auditing has been more important and relevant….

The Institute of Internal Auditors (IIA), the governors of the profession, tried to keep on track with these changes in the business environment. In 1999 (IIA n.d.(a)) a change in the internal audit profession was initiated by developing the current definition and updating the Professional Practices Framework (PPF) – (IIA 2006(a)). In 2009 (IIA 2009(a)), this document was further updated for the global profession, namely the International Professional Practices Framework (IPPF), including the Standards for the Professional Practice of Internal Auditing (hereafter referred to as *Standards*). This current definition was developed to encompass all the dimensions of 'modern' internal auditing, suggesting a profession that is characterised by broad business parameters and technical skills (IIA 2009(a):2):

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Internal auditors are not only seen as the right hand of management in assuring that policies, plans and procedures are adhered to (traditionally called assurance services), they now also, according to the revised definition of internal auditing, fulfill a consulting role (the new role is debated in Chapter 2 in great depth). This is supported by numerous studies performed on the role, activities performed and responsibilities of the internal audit function (Krogstad, Ridley & Rittenberg 1999:27; Nagy & Cenker 2002; Deloitte & IIA (UK and Ireland) 2003; McCaul 2006(a):35; Campbell *et al.* 2006:45). This new role brought about greater opportunities for internal auditors as their sphere of activities broadened. They are seen as part of the management team and are frequently asked to assist with decision making. They play a significant role in corporate governance processes, as demonstrated by the recent third King Report (IOD 2009:93), including the investigating of, and reporting on, crucial aspects such as business risks threatening the achievement of organisational objectives.

With these opportunities come responsibilities. Management has certain expectations of internal auditing, including a supporting role in the monitoring and improvement of risk management, internal control and corporate governance processes (Sarens & De Beelde 2006(a):163). Although providing assurance to management on the control activities has always been a part of the internal auditor's job description, risk management and corporate governance is a relatively new field for the profession (refer to table 2.2 on p. 71 where the previous and the current definition of internal auditing are compared). Internal auditors need to understand the concept of risk management as well as what is expected from them regarding this concept. They need to understand how risk management affects their activities, both their current activities and in the future. They need to understand the organisation's environment to be able to know

which risks could threaten the reaching of strategic and operational objectives, and how these risks could be minimised. This will ultimately have an effect on how internal audit engagements are performed.

With the broadened role of internal auditors in mind, it is clear that the way internal audit engagements have been performed in the past needs to be revisited. A more streamlined approach is needed where internal auditing adds value by focusing on risks threatening the organisation, whilst continuing to provide management with assurance on the effectiveness and efficiency of the control activities, all within the framework of corporate governance.

With these changes in and challenges facing the business environment as well as the internal audit profession, this chapter is dedicated to providing the background to this study and hence the reasons why it is necessary. The chapter first addresses information on the changing internal audit environment, the development and challenges within the corporate governance sphere, the external audit profession's view of its co-profession, internal auditing in the private and the public sectors, and the need to alter the internal audit methodology, including risk-based internal auditing. Secondly, the rest of the chapter is dedicated to explaining the research methodology that is followed in the study to address the research problem.

1.2 THE CHANGING INTERNAL AUDIT ENVIRONMENT

Many factors, past and present, play a role in how internal auditing is perceived by various stakeholders, and ultimately, utilised by those stakeholders. These factors include (Hermanson & Rittenberg 2003:38-39; Spencer Pickett 2003:22-37; Dimma 2006:13-22; Van Wyk 2009:5):

- corporate governance scandals and the increasing corporate governance guidance, rules and regulations;
- organisational ('man-made') and environmental disasters;

- the never-ending battle between cutting costs and increasing quality (due to competition);
- new developments, systems and technology;
- complexity of the business environment, for example, technology, globalisation, skills shortages;
- changes in organisational ownership;
- ethical and legal pressure; and
- social responsibility and sustainability.

The above factors all influenced the need for change in modern internal auditing. In this section, some of the most important contributing factors with regard to the changing internal audit environment and how this change has taken place are discussed. The discussion includes the structuring and global play field of the profession, the growth in the number of competent and skilled internal auditors, the scarcity of certain skills, as well as guidance issued by the IIA. Section 1.3 on p. 12 addresses the influence of corporate governance and corporate scandals.

1.2.1 Brief background to the structure and globalisation of the internal audit profession

It is first important to understand the structure of the IIA as the governing body of the internal audit profession and how it can add value to organisations from a global perspective. Internal auditing is a global profession with the Certified Internal Auditor (CIA) designation being recognised worldwide. The IIA Incorporated (Inc.), or the global head office, is situated in the USA. The IIA Inc. plays an overseeing role for the various chapters of the IIA. It also hosts all international activities that cut across individual countries, for example, the global board meetings, international IIA staff meetings, and twice a year, international committee meetings where important decisions are made that feed into the various formal IIA guidance (IIA n.d.(b)).

Countries have chapters, affiliates, and/or regional offices, for example, in the USA there are forty-eight chapters with between one to eleven affiliates per

chapter (IIA n.d.(c)). The SA chapter has thirteen regions across Southern Africa (IIA (SA) 2008). All these bodies report at various levels to the IIA Inc. Although each operates as an individual unit, certain minimum requirements remain the prerogative of the IIA Inc. For example, although the IIA (SA) may decide on the criteria for determining who may sit for the CIA examination in SA, the IIA Inc. has determined a minimum requirement globally, namely a bachelor's degree or educational equivalent (IIA n.d.(d)). It is thus understandable that, although all formal guidance is the responsibility of the IIA Inc., many IIA bodies globally have developed their own guidance that is more specific to their country's circumstances and needs.

The above information strengthens the fact that the IIA is in the ideal position to assist internal auditors that are participating in the global business environment. Also, the IIA with its chapters and affiliates worldwide ensures that internal auditing remains globally competitive yet locally relevant.

1.2.2 Growth within the profession

The profession has seen enormous growth over the past years. Although the IIA is the governing body of the profession, not all individuals practising as internal auditors may register with the IIA. The criteria for registration differ from one country to another, but in short, a minimum requirement is a bachelor's degree or equivalent at a recognised institution with suitable experience (IIA n.d.(e)). Thus, to become a member of the IIA would mean that an individual has some form of tertiary education and this could be interpreted as the first step in the training of a competent internal auditor. It could be argued that most internal auditors who qualify for membership would want to register as this brings about various advantages (IIA n.d.(e); IIA (SA) n.d.(b)), including professional recognition, access to guidance material and continuous professional development information, entry to sit for the CIA examination, and many other benefits. Therefore, membership of the IIA could be a reasonable indication of practising competent internal auditors in the business environment. Table 1.1 on p. 7 provides a summary of IIA membership since 2000 (Erasmus 2009; Ttappous 2009(a); IIA n.d.(g); Johnson 2009). These statistics are echoed by a study

performed in SA on the demand for internal auditing in the country (iKUTU 2009:102-103), indicating a material number of vacancies in participating organisations as well as a further future demand projected.

Table 1.1: Summary of membership and certified internal auditors globally and in South Africa

	2000		2002		2004		2006		2008	
	M(*)	**CIA**	**M**	**CIA**	**M**	**CIA**	**M**	**CIA**	**M**	**CIA**
IIA Inc.	70993	33207	82147	40212	99433	50816	135500	64453	164896	74305
%growth	-	-	16%	21%	21%	26%	36%	27%	22%	15%
IIA (SA)	1305	154	2117	248	2725	447	4622	739	5819	935
%growth	-	-	62%	61%	29%	80%	70%	65%	26%	27%

(*)M – membership *(Source: refer to discussion)*

Although the statistics indicate a steady increase in the growth of the membership figures as well as of the number of CIAs, and this could be interpreted as a sign of growth within the profession, a few questions remain unanswered. Firstly, why are less than 50% of IIA members across the globe CIAs (and even less so in SA)? The CIA designation is the only globally accepted certification for internal auditors and remains the standard by which individuals demonstrate their competency and professionalism in the internal audit field (IIA n.d.(d)). A fair statement would be to conclude that the CIA designation is a reflection of the competency of internal auditors; this, again, reflects on the quality of activities performed by internal auditors. Secondly, why is there still a shortage of certain skills within the internal audit profession (refer to section 1.2.3 on p. 8)? Is this a sign that the potential growth rate could exceed the current growth rate if the IIA could meet the needs of the market, or is the IIA not attracting the right type of skilled people as members, thus fostering an artificial growth rate? Thirdly, could it be that corporate scandals, and the requirements according to corporate codes and legislation that pursued the scandals, are keeping the quest for internal auditors artificially alive? Or is it possible that management is accepting internal auditors as part of the team and truly believes that they could add value and make a difference in the organisation achieving its objectives?

It is not the aim of this study to answer all these questions, but it is to focus on casting light on aspects such as the growth in the competencies and skills needed for internal auditors to add value in the fields of corporate governance, and more specifically, risk management. The study also reflects on the way internal audit engagements should be performed as a result of this growth, namely being more productive and focusing on the crucial aspects at hand.

1.2.3 Scarcity of competent internal auditors

According to an international survey performed by Grant Thornton (2010) of medium to large private organisations, one of the major constraints for growth is the lack of availability of a skilled workforce (global – 25% and SA – 17%). With regard to internal auditors, although the statistics in table 1.1 on p. 7 indicate that there is a steady growth of IIA membership, with the changing role of the internal auditor the scarcity of competent and skilled people to perform the duties expected by management became an obstacle for the internal audit function (McCaul 2006(b):19; IIA Research Foundation 2007:282,290,308,325; PWC 2007:30-31; Ernst & Young 2007:8; Roffia 2007:14; Deloitte & IIA (UK and Ireland) 2008:6-7; PWC 2008(a):28-30; PWC 2008(b):39). The statistics in table 1.1 corroborate this statement as the number of CIAs compared to IIA members is very low (refer to section 2.6.3 on p. 119 for a further discussion). The results of a study performed in SA on the standing of internal auditing in publicly-held companies, the iKUTU study (2009:12), further supports this problem with the number of Chartered Accountants in SA (CA(SA)) that are appointed as chief audit executives (46.7%) compared to those holding the CIA qualification (30%).

Areas where there is a shortage of skilled internal auditors include, *inter alia*, (Robert Half International 2007; Ernst & Young 2007:6-9; IIA Research Foundation 2007:345) the fields of information technology (IT), governance related topics, and risk management (refer to section 2.4.3 on p. 79). The positive side to the shortage of skills is that it is an indication that management is utilising internal auditors to assist them with their responsibilities – thus 'trusting' them. On the negative side, if competent and skilled individuals are not available within the internal audit function, either management will turn to other resources available

within the organisation, or they will be dissatisfied with the work performed by the internal audit function. Both of these could harm the perceptions that management has of internal auditing.

1.2.4 Guidance issued by the Institute of Internal Auditors

The IIA has tried to keep abreast of the changing needs of the business environment and numerous formal and informal guidance documents have seen the light since 1999. The following is a list of the documents that are most relevant to this study (some of these are discussed in greater length in later chapters):

1.2.4.1 International Professional Practices Framework (IIA Inc.)

Structural guidance is needed to keep up with the pace of the changes to the business environment and hence to the internal audit profession. After the current internal audit definition was proclaimed in 1999, the need for a structural format for the different elements of professional guidance was identified. The IIA Inc. has developed guidance in the form of the Professional Practices Framework (PPF) and more recently the IPPF. The IPPF consist of six elements (IIA 2009(a):iv,xvi-xvii). Some of these elements are mandatory, for example, the code of ethics and the *Standards.* Other guidelines are merely strongly recommended (refer to section 2.4.4.1 on p. 81).

With reference to this study, the IPPF plays a dual role. Firstly, it is used for the guidance that it provides for internal auditors with regard to corporate governance and risk. Secondly, the study's outcome, namely a tool for internal auditors when performing risk-based internal audit engagements could possibly be incorporated in the IPPF as a practice guide.

1.2.4.2 Common body of knowledge (IIA Inc.)

The IIA Inc. recognised the need for competent and skilled internal auditors and in 2006 a research report on the revised Common Body of Knowledge (hereafter

referred to as CBOK) was produced (IIA Research Foundation 2007). This global study addresses the compliance of internal audit functions with the *Standards,* how internal audit functions operate, and emerging trends and roles of internal auditing (IIA Research Foundation 2007:2). The questionnaire was circulated to all IIA members worldwide and a response rate of 10% (IIA Research Foundation 2007:23) was obtained. The results of the CBOK study will be briefly discussed to cast light on the new trends within the profession with regard to corporate governance and risk management.

1.2.4.3 Competency framework (IIA Inc.)

As a result of the CBOK project, the IIA Inc. acknowledged the need to update the Competency Framework for Internal Auditors (hereafter referred to as CFIA). This document outlines the minimum level of knowledge areas and skills needed by internal auditors to be able to perform all the needed activities within an internal audit function. It is divided into interpersonal skills, tools and techniques, internal audit standards, theories and methodologies, and knowledge areas (IIA n.d.(f)). The areas relevant to corporate governance, risk management and risk-based internal auditing are investigated in the various chapters addressing these topics to identify the competencies required by internal auditors.

1.2.4.4 Institute of Internal Auditors position paper: Organisational governance – guidance for internal auditors (IIA Inc. & IIA (Australia))

This document (IIA 2006(b)) provides guidance on the key aspects of corporate governance (also referred to as organisational governance), the role of internal auditing, practical examples, and guidance issued by various stakeholders. This document is further debated in Chapter 4 of the study.

A further document issued by the IIA (Australia) in conjunction with the IIA Research Foundation and the RMIT University in Australia (Leung, Cooper & Robertson 2003) was the result of a research study that evaluated the role of internal auditing within corporate governance and management. The report

addresses the accountability structure and objectives of the internal audit function, the nature of the duties to be performed, and the relationships of the internal auditor within the corporate governance sphere.

1.2.4.5 Institute of Internal Auditors position statement: The role of internal auditing in enterprise-wide risk management issues (IIA (UK and Ireland))

The IIA (UK and Ireland) issued a statement to compliment the *Standards* on the role of internal auditing regarding risk management. This document was later adopted by the IIA Inc. (IIA 2004). The document suggests the idea of internal auditing playing a core role in evaluating as well as providing assurance on the risk management process, providing assurance that risks are evaluated correctly, evaluating the reporting of key risks, and reviewing the management of key risks. This document is further debated in Chapter 4 of the study.

1.2.4.6 Institute of Internal Auditors position paper: Risk-based internal auditing (IIA (UK and Ireland))

The IIA (UK and Ireland) (2003) issued a statement on risk-based internal auditing as a result of the changes over the last few decades in internal audit activities. The document sets a guideline for internal auditors when adapting their internal audit approach to a risk-based approach. It emphasises the fact that risk maturity is crucial for the successful implementation of this internal audit methodology. This document is further debated in Chapter 4 of the study.

1.2.4.7 Application of the guidance

Although the IIA has developed much guidance on various areas, the question that remains is whether their members are using these guidelines in their daily activities. The CBOK study indicates that 85.5% of the respondents confirmed that their internal audit function do adhere to the *Standards* (IIA Research Foundation 2007:30), meaning 14.5% do not. Further, it could be argued that of the many internal auditors that did not complete the study (only 10% response

rate worldwide) some of these will also not adhere to the *Standards*. Further studies confirming the problem of non-adherence to the *Standards* include a study performed in Malaysia to determine whether organisations listed on the stock exchange complied with the *Standards* (Fadzil, Haron & Jantan 2005:844-866) as well as a study performed in Europe to determine the use of and adherence to the *Standards* (Burnaby, Abdolmohammadi, Hass, Sarens & Allegrini 2009:835-860). The *Standards* is a compulsory document (IIA 2009(a):iv). If internal auditors do not even adhere to a compulsory document, do they consult other guidance? This possible lack of interest not withstanding, guidance for all stakeholders and role players in the business environment is crucial. The IIA should continue keeping up-to-date with new trends and developments as well as providing guidance on these.

1.2.5 Conclusion

The internal audit profession has undergone many changes in the last few decades. With management expecting more from the internal audit function, the IIA positioned itself in such a manner that it can provide guidance to its global members. This has brought about a growth in not only the profession, but also in the membership of the IIA. Even so there is a scarcity of knowledge and competency in certain areas. This needs to be addressed as a matter of urgency or management could turn to other role players to assist them in these areas. The IIA must keep abreast of developments and provide their members with relevant guidance.

The aspect of providing relevant guidance is also applicable to the business environment. The formal structuring of sound corporate governance principles is one of these initiatives.

1.3 CORPORATE GOVERNANCE

The concept of corporate governance has developed over the years (Fama & Jensen 1983; OECD 1999; Solomon 2007; Van Wyk 2009) and is in short defined as the system by which organisations are directed and controlled, striving to

maintain a balance between the freedom of the management team, their responsibilities and the interests of relevant parties (OECD 1999:1; IOD 2002:20; Solomon 2007:77; ECGI n.d.). For the public sector, governance is the ability of a government to develop a public management process that will be able to make sure that the citizens of the country's money is spent wisely to ensure maximum service delivery (USA - Agency for International Development 1998; Halachmi 2005:302).

To demonstrate the importance of sound corporate governance principles, a study (Rose 2003:17) performed by the McKinsey Consulting Group announced that investors in emerging markets, such as the SA market, are willing to pay a premium of between 23% and 28% for shares in a company that implements good corporate governance principles.

In this section, the development of corporate governance codes as well as legislation is briefly discussed. It is important to note that the reason why corporate governance is included in this study is that both internal auditing as well as risk management is included in most corporate governance codes as two of the cornerstones of sound governance principles. Even with these developments, corporate scandals still occur. The most prominent corporate scandals and how these affected the internal audit environment are also mentioned. This is only a brief introduction to corporate governance – refer to sections 2.5.2 on p. 87, 3.2 on p. 138, 3.3 on p. 153 and 4.2 on p. 228 for a more comprehensive discussion as well as the effect of corporate governance on risk management and internal auditing.

1.3.1 Corporate governance codes

In the last three decades many codes and other guidance have been issued by governments, institutes and other regulators on the concept of corporate governance and related topics, for example, internal control and risk management. These all provide some form of guidance to management on how to improve structures, policies and procedures, rules, activities and processes, etc., of the organisation – thus, how to successfully manage an organisation.

According to the European Corporate Governance Institute (ECGI n.d.), sixty-four countries and five *ad hoc* bodies have issued corporate governance codes to provide organisations with guidance. Although many new corporate governance codes are issued on an ongoing basis, each new code adds to the evolution of the concept of corporate governance (refer to section 2.5.2 on p. 87 for corporate governance links to internal auditing and section 3.3.4 on p. 163 for its links to risk management).

In SA, corporate governance was introduced with the issuing of the first King Report on 29 November 1994 (IOD 1994), followed by the second report during 2002 (IOD 2002) and the third report in 2009 (IOD 2009). These reports contain a set of recommendations for sound corporate governance, including the topics of internal auditing and risk management; for example, the reports recommend the implementation of internal audit functions for various organisations. Although the corporate governance principles as set out in the reports are only recommendations, from 1 September 2003 (Baue 2003), all companies listed on the Johannesburg Stock Exchange, the JSE Limited, which is the SA stock exchange, must comply with the second King Report. King Report III (IOD 2009:17-18), effective from 1 March 2010, goes even further as the code applies to all organisations regardless of the manner and form of incorporation or establishment.

1.3.2 Corporate governance legislation

Governments and other regulators are beginning to understand the advantages of having an effective corporate governance strategy. In SA, after the first King Report (IOD 1994), the government followed suit and since 1999, much legislation has been promulgated that focuses on sound corporate governance principles. After major scandals occurred in the USA, their government proclaimed legislation to try and mitigate the risks. Many such examples exist and those most relevant to this study are briefly discussed.

1.3.2.1 South African legislation on corporate governance

The public sector promulgated the Public Finance Management Act (SA – No 1 of 1999 as amended by Act No 29 of 1999), hereafter referred to as the PFMA, and the Municipal Finance Management Act (SA – No 56 of 2003), hereafter referred to as the MFMA, both enforcing sound corporate governance principles for public sector organisations. The PFMA and MFMA have as their main objective (SA – 1999:S2; SA – 2003:S2) the regulation of financial management to ensure that all revenue, expenditure, assets and liabilities of national, provincial and municipal government organisations are managed efficiently and effectively. The Treasury Regulation (SA – National Treasury 2005), which was issued in terms of the PFMA, underlines the principles stated in the PFMA.

The Protocol on Corporate Governance (SA – Department of Public Enterprises 2002:2) has the objective of providing guidance for state-owned enterprises on proper governance and control. The PFMA (SA – 1999:S50-51), MFMA (SA – 2003:S82,S121) and Protocol on Corporate Governance in the Public Sector (SA – Department of Public Enterprises 2002:5) address the concepts of accountability of government organisations and the transparency of systems. Internal auditing is in the perfect position to assist the government with this task. Therefore, both internal auditing and risk management are included in the legislation.

In 2005, the SA Department of Trade and Industry embarked on a process to overhaul and update the Companies Act, No 61 of 1973. The process was executed in two phases, namely the Corporate Laws Amendment Act (SA – No 47 of 2007) that came into effect on 14 December 2007, and the Companies Bill (SA – No 61B of 2008) that entailed a complete and more complex review of the Companies Act. The Bill has been replaced by the new Companies Act (SA – No 71 of 2008) that has been promulgated on 9 April 2009 and it is expected that it will be put in operation during 2010 (SAICA 2010). According to Section 94 of the Companies Act, companies must now appoint an audit committee, a step in the direction of enhancing the importance of corporate governance.

1.3.2.2 United States of America legislation on corporate governance

The biggest consequences of the Enron scandal is that in 2002, the USA Congress passed SOX (USA – 2002), the

> …most major and radical set of financial auditing changes in the USA since the 1930s (Moeller 2002:3).

As Enron's failure, and WorldCom's to a smaller extent, was directly linked to financial statement fraud and the role that the external auditors played, the Act is a set of new rules for organisations, encompassing auditor independence to corporate responsibility and financial disclosure, to name a few areas.

Although corporate governance guidelines are a necessity for boards and managers to survive in the ever-increasingly complex business environment, the question arises whether this should include total control in the form of regulations and legislation. With the issuing of the Sarbanes Oxley Act, 2000 (hereafter referred to as SOX), a strict rule-based approach, precisely this was done. Since then, many have argued the principle *versus* rules debate (Barrier 2003:68-73; Jackson 2004:56-60; Markham 2006:661-663). Refer to section 3.2.3.3 on p. 149 for a discussion of this topic.

A last fact relevant to this study and the implementation of sound corporate governance principles, is that all companies listed on the New York Stock Exchange (NYSE) are required to have an internal audit function, with the audit committee overseeing the function (IIA n.d.(h)).

1.3.3 Corporate governance in other countries

The following is a summary of some of the countries where corporate governance principles have been successfully incorporated (IIA n.d.(h)):

- Australia – All companies listed on the Australian Stock Exchange must have an audit committee.

- Canada – All government agencies must have an audit committee.
- India – All listed companies must have an internal audit function.
- Kenya – All listed companies must have an internal audit function.
- Malaysia – All listed companies must adhere to the Malaysian Code of Corporate Governance.
- Netherlands – All public sector organisations are required to have internal audit functions.
- Sweden – Swedish government agencies must establish an internal audit function.

1.3.4 Corporate scandals

Major corporate scandals and accountability failures that occurred in recent years have led to corporate collapses that harmed thousands of stakeholders – from shareholders and other external parties, to employees and pensioners (Van Wyk 2009:3). Although corporate scandals are not new phenomena (Spencer Pickett 2003:37), the intensity with which the business environment has been influenced, is on the increase.

One of the biggest corporate collapses in the history of the world is Enron (Spencer Pickett 2003:42-43; O'Brien 2005:205-206; Markham 2006:49-142; Williams 2008:471-473), America's seventh largest company, situated in Houston, that went from being worth $60 billion to bankruptcy. The collapse occurred as a result of its complex trading activities and financial manipulation and was an accounting scandal. Being one of the 'Big 5' audit firms at that time in the world, Arthur Andersen was both the external as well as the internal auditors of Enron. In 2000 they earned $52 million in fees from Enron of which $27 million was internal audit fees and $25 million external audit fees (Markham 2006:205) – compromising its independence. As the external auditors, Arthur Anderson had given unqualified audit opinions on Enron's annual financial report of 31 December 2000, the year the scandal was revealed (Markham 2006:197). After the whole Enron debacle was unravelled, it was argued that the auditors could not have been in the position to issue unqualified reports. It was also argued that

the internal auditors were in the perfect position to identify the problems and risks. The result was that Arthur Andersen had to close its doors.

The USA's economy was still trying to recover from the blow that Enron handed out when a second major scandal hit the country, namely WorldCom (Spencer Pickett 2003:43; Markham 2006:311-376; Cooper 2008). The WorldCom scandal was also an accounting scam where corporate expenses were being treated as capital investments, thus inflating the profit of the organisation by $3.8 billion. Again it was the internal auditors that were associated with the scandal, but contradictory to the Enron debacle, Cynthia Cooper, the chief audit executive uncovered the fraud. The result was that WorldCom went bankrupt and a whole town went under.

Although Enron and WorldCom are seen by many as the biggest scandals in the corporate world, especially as both occurred in such a short time-span and so affected the USA market, many other such falls have occurred before and afterwards. The managing director of a United Kingdom (UK) based personnel placement firm, Executives Online, Norrie Johnston stated that

> …companies now realize that these kinds of scandals do not just happen in the US… (Anonymous 2004:7).

In SA, many scandals have affected the business environment, for example, LeisureNet in 2001 (SAPA 2007(a)) and Fidentia in 2007 (SAPA 2007(b)). Probably one of the most controversial scandals that is still an on-going concern is the arms deal, a public sector procurements transaction. In 1995, the government purchased US$4.6 billion worth of weapons. Unfortunately many allegations of corruption have been linked to this transaction, including bribery by and from various high-level political figures (Feinstein 2007; Southern African Information Portal on Corruption n.d.). According to Lubbe (2008(a):28-29), the government of SA is at a crossroad when it comes to fraud and other irregularities. He argues, with underlying proof, that many politicians have little respect for legislation. This is a breeding ground for the committing of fraud, both by politicians and government employees. Employees argue that if management can commit fraud and justify it, they may also. This has a snowball effect and the

general public argues that if government gets away with fraud, the individual may also. This is echoed by Mervyn King for the private sector (Barrier 2003:71) as he claims that:

> …fish rot from the head. Companies need to set a standard at the top, and if those at the top start acting wrongly or unethically, the whole company knows about it.

It can be concluded that most corporate scandals have a few basic elements in common, or rather, more accurately, a lack of certain elements in common. According to O'Brien (2005:22) and Markham (2006:108) the most prominent factors that led to the scandals include, *inter alia*, ineffective governance systems, and inadequate oversight and accountability actions of the board of directors. In response to these and other factors, major reforms have been implemented worldwide to assist management and other role players in preventing these types of scandals. These and other scandals and their effect on the implementation of a risk management framework (refer to section 3.2.3.1 on p. 146) and/or internal auditing (refer to section 2.5.2.4 on p. 103), are discussed in later chapters.

1.3.5 Conclusion

The above discussions clearly indicate that corporate governance is being viewed anew and from a different perspective by different parties. Various parties are constantly developing new guidance in the form of corporate governance codes and other relevant documents. Governments incorporate guidance for the public sector in the form of legislation. Although these principles do not prevent corporate scandals from occurring, it could be argued that without the guidance, many other scandals would have occurred. Corporate governance is a principle-driven concept that focuses on implementing certain activities or functions that will assist management with the directing and controlling of the organisation. Two of these are the external auditors and the internal auditors, both will be discussed hereafter.

1.4 EXTERNAL AUDITORS

Both external auditors and internal auditors play a crucial role in the success of the governance of an organisation and are seen by many corporate codes as two of the cornerstones of sound corporate governance (Turnbull Report 1999:par 42-47; IOD 2002:86-89; Basle Committee 2004:principle 4). Thus, how the external auditors perceive the internal audit function could influence the view that management has of the internal audit function, and ultimately the utilisation of the function and the seriousness with which management views its activities. With this in mind, the external audit profession is facing its own problems, with specific aspects such as the profession's involvement in recent corporate scandals (refer to section 1.3.4 on p. 17) and the challenges of maintaining stakeholders' trust and integrity, as well as general aspects such as globalisation and the increasing complexity of the accounting and auditing field.

Although there are many differences in the methodology, structure, roles and responsibilities of the two professions (refer to section 2.3.1 on p. 64 for a detailed discussion), the external audit profession realises that it could benefit from utilising internal auditing on aspects such as obtaining a better understanding of the organisation and its specific environment, as well as relying on certain activities performed by the internal auditors.

1.4.1 Guidance on the external auditors' use of the work of the internal auditor

The *Standards* (IIA 2009(a):27,101-103) do address the coordination between the two professions, but for the purpose of this discussion it is more important to understand whether the external audit profession will rely on the work performed by the internal audit function. According to the International Standards on Auditing (ISA) 610 (SAICA 2009/10) the external auditors may rely on activities performed by the internal auditors, provided certain criteria is met (refer to section 2.5.3.2.2 on p. 110 for a discussion). One of these criteria is that the external auditor should evaluate the work performed by the internal auditor on a specific internal audit engagement that the external auditor wants to rely on. This

relationship could thus also benefit from a structured risk-based internal audit engagement.

Although the coordination is a strengthening of governance principles and a cost saving exercise, the proof of whether this actually does happen lies in the practical application of the guidance as set out by the external auditor's regulatory bodies.

1.4.2 The external auditors' use of the work of the internal auditor

Early studies that have been performed on the use of the internal auditor's work by the external auditor (Wallace 1984; Reinstein, Lander & Gavin 1991:29-36; Gramling 1999:117-135;) all conclude that although the latter uses the work performed by the internal auditor, the most significant reason is the fee pressure imposed by the audit client. A more recent study performed by Haron, Chambers, Ramsi and Ismail (2004:1148-1159), questioning sixty-four external auditors, reflects a different view. The most important factors influencing the judgement of the external auditor are the internal auditor's training (competency) and the satisfactory follow-up procedures performed in previous audit engagements (scope of activities). Both these factors encourage organisations to appoint competent and properly trained internal auditors, and management to consider carefully before interfering with the scope of the internal audit function's activities. The complementary effect that internal auditing has on the external audit fees is also confirmed by other recent studies (Goodwin-Stewart & Kent 2006(a):387-404; Singh & Newby 2010:309-327).

1.4.3 External auditing for the public sector

In SA, the Auditor General is established in terms of the Constitution of South Africa (SA – No 108 of 1996:S181(1)(e)) to enhance oversight, accountability and governance for the public sector; thus fulfilling the role of the external auditor for all government organisations. The Constitution as well as the Public Audit Act (SA – No 25 of 2004:S4) set out the functions of the Auditor General. With regard to internal auditing, according to the PFMA (refer to section 2.5.2.3.2 on p. 102),

all government organisations must have an internal audit function. Therefore, as for the private sector, it would benefit both the Auditor General as well as the internal audit function if these two parties could work closely together and rely on one another's work performed. However, statistics reveal otherwise. According to the national general report of the Auditor General, one of the areas that were identified as the cause of audit reports being qualified is the ineffectiveness of the internal audit function. Unfortunately not all the information could be obtained from the Auditor General's data base (Matsi 2009), but the results of the 2007/2008 provincial government audit reports revealed that in at least two provinces, namely Free State and Northern Cape, the ineffectiveness of the audit committee and internal audit function was highlighted as a root cause for the qualification (refer to table 1.2 on p. 23). Furthermore, in three other provinces, inadequate governance arrangements are indicated as a root cause for qualification, which could include the internal audit function and/or risk management framework.

1.4.4 Conclusion

In the modern business environment, the pressure is increasing for organisations to lower their costs and spend money more wisely. One of the areas where organisations could save is to ensure that there is little or no duplication of the work performed by the external and the internal auditors. This would bring about a cost saving in the external audit fees. Management needs to know that this will only happen when they appoint competent internal auditors that perform activities according to a structured and acceptable methodology, for example, a risk-based internal audit approach.

In the following section, the internal audit profession in the private and the public sectors are compared to determine whether the study could and should include both.

Table 1.2: Audit reports for the provincial government for the 2007/2008 financial year

Province	Type of audit opinion					Root causes(*)
	Adverse	Disclaimer	Qualified	Unqualified (with matters)	Unqualified (without matters)	
Eastern Cape	16%	0%	38%	46%	0%	• Inadequate governance arrangement
Free State	0%	0%	42%	58%	0%	• Ineffective audit committee • Ineffective internal audit • Ineffective internal control • Inadequate governance arrangement
Gauteng	0%	0%	14%	79%	7%	
KwaZulu-Natal	0%	0%	19%	75%	6%	
Limpopo	0%	0%	61%	31%	8%	• Inadequate governance arrangement
Mpumalanga	0%	0%	38%	62%	0%	
Northern Cape	0%	17%	33%	50%	0%	• Ineffective audit committee • Ineffective internal audit
North West	0%	8%	38%	38%	16%	• Inadequate governance arrangement
Western Cape	0%	0%	8%	77%	15%	

(*) Only root causes linked to this study *(Source: AGSA 2009(a):12-17)*

1.5 INTERNAL AUDITING IN THE PRIVATE AND THE PUBLIC SECTORS

This study incorporates both the private and the public sectors. It is thus appropriate to investigate the reason why both sectors are included by examining the differences and similarities within these two sectors with regard to the internal audit profession, including corporate governance and risk management.

Before this can be done, it is important to set boundaries for each sector. For this study, private sector organisations include all organisations that are fully or partially privately owned, including public-owned companies, private-owned companies, closed corporations, partnerships and sole proprietaries. For SA, Schedule 2 public entities as classified by the PFMA (major public entities) are also included as many of these are listed on the JSE Limited. Public sector organisations include all organisations that are governed or partially governed by the government. For SA (South African Government n.d.), this includes all thirty-seven national government legislatures that were in place before the 2009 elections, the nine province's provincial government legislature, two hundred and eight-three local government legislatures, and Schedule 3 public entities as classified by the PFMA ('other' public entities).

Words that can be used for all the different types of businesses in both these sectors include entities, companies, organisations, corporations, institutions, etc. For the purpose of consistency, all the above will be referred to as 'organisations'. This word was chosen as it is regarded by many dictionaries and experts (Swanson & Marsh 1991:40; Cole 2004:8; Oxford Dictionary 2005:820; Du Plessis 2009(b); Wikipedia n.d.(d)) as the most inclusive term used to describe all different types of businesses, both in the private and the public sectors. It is also the word chosen by the IIA to be used in their formal guidance, namely the IPPF (IIA 2009(a)).

1.5.1 Differences

Seen from a business environment perspective, the private and the public sectors function differently (Du Toit, Knipe, Van Niekerk, Van der Waldt & Doyle 2002:17-

19; Pauw, Woods, Van der Linde, Fourie & Visser 2002:1; Van der Waldt & Du Toit 2005:46). For example, the main objective of any private sector organisation is to make a profit for its shareholders. The main objective of a public sector organisation is to deliver a service to the public, thus serving the country and/or community. Carhill and Kincaid (1989:51-52) underline the above by identifying two major factors influencing the differences within the two sectors, namely the fact that government is mainly driven by legislation whereas the public sector is more outcome-driven; and the public sector is service-orientated whereas the private sector is profit-driven. They argue that these differences could have an effect on the internal audit environment. It is further debated that internal auditing in the private and public sectors could differ substantially as a result of factors such as governments operating within different cultures, for example, Asian, Western or African cultures fostering different ethical norms, legislation that differs, and the organisational status of internal auditing within a specific government organisation (Carhill & Kinciad 1989:50; Coupland 1993:4; Goodwin 2004:640; Van Gansberghe 2005:70; Sterck & Bouckaert 2006:50).

It could, however be argued that all the above could also be true for the private sector. Firstly, no two private sector organisations operate the same way; even two organisations within the same sector will have prominent differences in their operations, policies, procedures, regulations, etc. Secondly, legislation for private sector organisations also differs from one sector to the other, for example, the Bank Act that is only applicable for certain financial institutions. Lastly, internal auditing base their activities on principles, and aspects such as cultural differences linked to ethical norms as well as organisational status are inferior thereto, for example, a medical doctor operating in a government hospital will use the same methodology to perform his task as a doctor operating in a private hospital. Other factors may differ, but the doctors' procedures and ethical principles will remain the same.

Goodwin (2004:643-648) explores the differences and similarities between internal auditing within the public and the private sectors and identifies five prominent areas where significant differences are found. Two of these differences could have an effect on the outcome of this study, namely the status of the

internal audit function within the organisation, and retaining internal audit personnel.

The status of internal auditing within the organisation (refer to section 2.6.1 on p. 113) determines the importance and independence of the function. It thus plays an important role in determining whether the findings of audits performed and the recommendations of the internal auditors are taken seriously by management. Goodwin (2004:643) measures the status of internal auditing by reporting lines and consistency of internal auditors. Global studies indicate that internal auditors within the public sector mainly (57% – Goodwin 2004:644) report to the chief executive officer and the audit committee (Eckhart, Widener & Johnson 2001:52; Wynne 2001:1; Sterck & Bouckaert 2006:50), with all chief audit executives in SA organisations included in a study performed by Van der Nest in the public sector reports to the audit committee (2006:196).

Goodwin (2004:643) reports that chief audit executives in the private sector report to various senior management positions with numerous other studies producing contradictory results (refer to section 2.6.1 on p. 113). Studies in SA performed in the private sector confirm this tendency. A study performed by Marx (2008:433) on audit committees in larger listed companies concluded that audit committees do review the findings of the internal audit function. In a further study (iKUTU 2009:25,30) amongst executives of the top forty companies listed on the JSE Limited, the majority of the audit committee chairpersons as well as the chief executive members interviewed confirmed this fact with reporting lines to the chief financial officer, chief executive officer, chief operating officer, and chairperson of the board, to name a few. This could undermine the independence of the internal audit function, especially when reporting lines include the chief financial officer and chief operating officer. Internal auditors' main investigating activities include the areas for which these two positions are responsible. The question asked is would the internal auditor report problems to his/her superior to which they are responsible?

Permanent internal auditing positions (Goodwin 2004:644), as opposed to internal auditing being used as a stepping-stone, are more favoured (94% in the

public sector and 67% in the private sector) in the public sector. Thus, for the public sector, after attracting the right mix of competent and knowledgeable personnel, these people will probably be able to contribute more to the internal audit function. In the long term, this should better the quality of the output of the internal audit functions in the public sector.

1.5.2 Similarities

Not withstanding these differences between the two sectors, a very important overlap between the private and the public sectors' administration and management exists. Both have the same main purpose, namely the reaching of their objectives (Du Toit *et al*. 2002:24). According to the definition of internal auditing, one of the main tasks of the internal audit function is to assist management with this task (IIA 2009(a):2). This has a direct influence on the way internal audit duties are performed and has no link to a specific sector.

Additionally, as with internal auditing in the private sector, the internal audit function of government organisations must add value (refer to section 2.4.1.2 on p. 73 for a discussion). For the private sector this will entail assisting management in running the organisation according to sound governance principles and thus promoting an increase in shareholders' value. For the public sector it entails the contribution to better service delivery. Both these goals can only be obtained through identifying and managing risks, establishing effective control systems and maintaining sound governance and business practices (Carhill & Kincaid 1989:51; Coupland 1993:4; Lapointe 2004:64-66; Van Gansberghe 2005:70). This also has a direct influence on the way internal audit duties are performed.

Goodwin (2004:645) identifies a further similarity between the two sectors relevant to this study, which is also confirmed by other studies, namely the nature of internal audit duties, specifically the involvement of internal auditing in risk management (Wynne 2001:3; Subramaniam, Ng & Carey 2004:90; Van Gansberghe 2005:71). This study identifies that although internal auditing within the private sector spends slightly more time (Goodwin 2004:645-646) on risk

management (18%) than the public sector does (15.5%), both these sectors spend a substantial amount of time on strategic risks, as these are an increasing concern for management (Drew, Kelley & Kendrick 2006:127).

1.5.3 Legislation and other regulations

Although there may be differences as well as similarities in the activities performed by and duties of internal auditing in the private and public sectors, certain regulation is applicable to both sectors. Firstly, compliance with the IPPF is a necessity for all who perform internal audit activities – both private and public sector organisations (IIA 2009(a)). Secondly, corporate governance codes are applicable to both these sectors, for example, the King reports in SA where the second report even refers to the PFMA and MFMA in the application of the code (IOD 2002:21).

As the government operates within a strict legal structure, a sound framework for internal auditing is needed to ensure that the IPPF, especially the *Standards*, as well as corporate guidance are being adhered to (Carhill & Kincaid 1989:51-52; Eckhart *et al.* 2001:52; Van Gansberghe 2005:72-73). For example, in SA, an effective and efficient internal audit function (refer to section 2.7 on p. 130 for a detailed discussion) within government organisations (SA – 1999:S76(38)(a)(ii); SA – National Treasury 2005:3.2), that reports to the audit committee, is compulsory by law (SA – 1999:S77; SA – National Treasury 2005:3.1). Other countries that have passed legislation governing the internal auditing for public sector organisations include, *inter alia*, the Netherlands, Sweden and the USA (Sterck & Bouckaert 2006:51).

This is not the case in the private sector in SA. No legislation enforces a private sector organisation to implement an internal audit function. The only form of compulsory requirements is for companies listed on the JSE Limited that have to comply with the King Report on Corporate Governance (refer to section 1.3.1 on p. 13 for discussion).

1.5.4 Conclusion

From the above it is clear that although there are some differences, there could be significant similarities between internal auditing within the private sector and the public sector. The way internal audit engagements are performed should be consistent – that is in accordance with guidelines set by the *Standards.* Furthermore, internal auditing is a principle-driven profession. This is eminent by the fact that the IIA has issued only a twelve-point Code of Ethics and twenty-three pages of *Standards*, these being the only compulsory guidance. Although operational processes, organisational policies and procedures, rules and regulations, and the general business environment in which internal auditors operate will have an effect on their activities, the internal audit process (refer to section 4.4.1 on p. 251 for a discussion) used when performing an internal audit engagement will not be influenced by these factors. Thus, a risk-based internal audit model that can be used to perform internal audit engagements should be applicable to both the private and the public sectors.

1.6 CHANGES IN INTERNAL AUDIT METHODOLOGY

The history of auditing, internal auditing and the evolution of the profession are briefly discussed in Chapter 2. For the purpose of introducing internal audit methodology, the changes that have brought about the need for risk-based internal audit engagements, as well as the way activities have changed, are introduced in this section.

1.6.1 Need for change

Originally internal auditing's role was to test the reliability of financial information. During World War I and II, cost effectiveness became more important and the internal auditors had to adapt to this new 'need' that management had (Sawyers, Dittenhofer & Scheiner 1996:19). Since the middle 1940s, this change was, and still is, a never-ending occurrence (refer to section 1.2 on p. 4 for a list of some of the most current factors enforcing change). Every time the business environment changes, management has to adapt to ensure that the organisation survives.

Internal auditing, as the right-hand of management, needs to adjust and provide a different or additional service to management. One of the areas where internal auditing adapted to the need of management is the incorporation of risk into the way internal audit engagements are performed.

1.6.2 Change in the way internal audit engagements are performed

Management is responsible for implementing internal control procedures that will minimise fraud and mistakes (IOD 2002:73-74; IIA 2009(a):111). The most common task of internal audit functions is to be the eyes and ears of management with regard to the adequacy of and compliance with these control procedures (Campbell *et al*. 2006:44). In the early years, this entailed performing 'internal check procedures' to ensure the adherence to internal control procedures. During the 1990s, management's vision when implementing internal control procedures shifted to focus more on areas where the risk for the organisation is high. The internal auditors had to adapt to this change and a new methodology for the activities of the internal audit function evolved, namely a risk-based approach (Spencer Pickett 2003:10-12). This new way of thinking is incorporated into various activities of the internal audit function, including the way internal audit engagements are performed.

Some of the literature during the 1900s (COSO 1992; McNamee 1997:23; Bank of Canada 1998:5-8; McNamee & Selim 1998:103-112; McNamee & Selim 1999:35) mentioned the term risk-based auditing for internal auditing purposes and shifted the vision of the internal auditor during an engagement. This entailed a paradigm shift from focusing on the adequacy of internal controls and the compliance to these control procedures, to focusing on the controls that can minimise the risks that threaten the operational objectives of the activity under review, as demonstrated by the first Committee of Sponsoring Organisations (hereafter referred to as COSO) model (refer to section 2.5.2.2 on p. 92).

When using the first model (COSO 1992) to perform an internal audit engagement, internal auditors had to (only a summary of the process):

- identify the objectives of the operational activity under review;
- scrutinise the risks threatening the achievement of these objectives;
- confirm that sufficient and adequate internal control procedures are implemented by management to minimise the risks to an acceptable level; and
- verify the operational activity's compliance with the internal control procedures.

After the success of the first COSO model, the committee identified the need for a formal risk management process. The second COSO model (COSO 2004) outlined the methodology for such a process to be implemented by management (refer to section 2.5.2.2 on p. 92). The process entails the (only a summary of the process):

- identification of risks;
- measurement of these risks with regard to the impact on the organisation and the likelihood of occurrence; and
- implementation of proper plans to minimise these risks to an acceptable level.

This second COSO model paved the way for management to begin a new level of managing risks within an organisation. Internal auditors, being the eyes and ears of management, are entering into a new phase with regard to risk management and its incorporation into the way internal audit engagements are performed. This is underlined by the fact that the recently issued third King Report (IOD 2009:15) identifies risk-based internal auditing as an emerging governance trend. Although the COSO Report (2004) focuses on the formal risk management process for the organisation as a whole, the question to be asked is whether this methodology can be used to streamline the risk-based internal audit approach when performing an engagement.

1.6.3 Conclusion

Change is the only constant in the world, especially in the business environment. Management needs to adapt to this constant variability. Internal auditing, being part of the management team and with the profession's main objectives to add value and assist management with reaching the organisation's objectives, has to keep up with these changes. One of these areas is the way internal audit engagements are performed, namely risk-based internal auditing.

1.7 RISK-BASED INTERNAL AUDITING

Before the concept of risk-based internal auditing can be investigated, it is important to understand the one factor that distinguishes it from other forms of internal auditing, namely 'risk'. The generic concept of risk, business risk, how it has evolved to the risk management process, and how internal auditing can use it to perform internal audit engagements, are discussed at great length in Chapters 3 and 4 of the study. The purpose of the next section is to briefly introduce the concepts of risk and risk management as the foundation of risk-based internal auditing.

1.7.1 Definition of risk

According to various dictionaries and other literature (Skipper 1998:6; SA – Public Service Commission 2003:7; IOD 2002:73; Valsamakis, Vivian & Du Toit 2005:26-27; Merna & Al-Thani 2005:7; Wikipedia n.d.(b)), risk is the possibility that an accident or a loss can occur, or a potential threat as a result of an uncertainty, or the loss of an opportunity. Various types of risks are identified, for example, stakeholder risks, reputation risks, legal compliance risks, ethics risks, project risks, global risks, elemental risks, holistic risks, contingent risks, and many more (Merna & Al-Thani 2005:17-25). In this study, risk is classified as business risk. The reason for focusing on business risk is that risk management and risk-based internal auditing focus on the risks threatening the achievement of an organisation's objectives within a specific business environment (refer to section 3.4.2 on p. 184 for a discussion of the term 'business risk').

According to PWC (1999:6), the King Committee on Corporate Governance (IOD 2002:73), the COSO Report (2004:16), Merna & Al-Thani (2005:9-10) and the Business Dictionary (2007/8), business risk is the threat that an event or action will have a negative effect on the ability of the organisation to achieve its business objectives and to execute its strategies effectively.

Business risk is thus summarised as an uncertainty whether something negative (hazard) or a loss of something positive (opportunity) that could prevent the organisation from achieving its objectives would happen or not.

1.7.2 Risk management as a cornerstone of corporate governance

In today's competitive world it is becoming increasingly difficult for organisations, both privately owned or in the public sector, to achieve good results. The possible reasons for this are the growing global market in which operations occur, scarce resources and constant changes in the business environment, to name a few. This greater and more complex market brings greater opportunities for organisations, which causes a greater risk for potential losses. Although management should limit this potentially hazardous effect on the organisation, it has to accept some measure of risk due to the fact that without taking risks, no gain will occur. To assist management with balancing these two extreme poles, namely limiting risks that will harm the organisation *versus* taking risks in order to grow, a structured process was developed, namely risk management.

For the purpose of introducing the concept, risk management is defined as the process of identifying, assessing, managing and controlling situations that may lead to the organisation not meeting its objectives (IOD 2002:73-75; Spira & Page 2003:642; COSO 2004:16).

Most parties involved in the business environment recognise that the responsibility for the risk management framework lies with the board and management for private sector organisations (IOD 2002:81-82; COSO 2004:83-84; IIA 2004), and the accounting officer for the public sector (SA – 1999:S38(1)(a)(i); SA – 2003:S62(1)(c)(i)). It is also evident from these

publications that an internal audit function is important for proper corporate governance, including the role it could play with regards to the aspect of risk management (IOD 2002:89; SA – National Treasury 2005:3.2.1,3.2.7; SA – 2003:S165(2)(b)(ii)).

Thus, to manage risk efficiently and effectively, management (and internal auditing as the assurance providers to management) should have an understanding of the concept of risk in general, the specific strategic and operational risks that threaten the organisation in particular, and the risk management process (IOD 2002:84; Spira & Page 2003:643; COSO 2004; Beasley, Clune & Hermanson 2005:530).

1.7.3 Internal auditing and the concept of risk

The role of the internal auditor regarding the management of risk within an organisation is influenced by the risk maturity of the organisation (IIA (UK and Ireland) 2003:3). For example, if an organisation is risk naïve (immature), internal auditing should promote risk management and rely on its own risk assessment to guide the function's activities. But if an organisation is risk enabled (mature), internal auditing should audit the risk management processes, and if applicable, use management's assessment of risks as appropriate during the audit process. Risk maturity is thus, in short, determined as the:

> …extent to which a robust risk management approach has been adopted and applied, as planned, by management across the organisation (De la Rosa 2008(b)).

Thus, the more relevant activities and elements of the risk management framework management have implemented effectively, the more risk mature the organisation is (RIMS 2006:4). This concept is discussed at great length in Chapters 3 and 4 of the study as it plays a vital role in the research methodology that is followed.

The IIA addresses the incorporation of the management of risk into the role that internal auditing should play within the organisation. The *Standards* identifies

three main areas where internal auditing should incorporate risk into their activities. For the purpose of this chapter, it is sufficient to conclude with a brief mentioning of the areas. These are investigated in more depth in section 4.3 on p. 232.

1.7.3.1 Risk management

The internal audit function should assist the organisation by identifying and evaluating significant exposures to risk, providing assurance on the adequacy of the risk management framework, specifically the risk management process, and contributing to the improvement of the risk management framework (IIA 2009(a):28-29,107-110; IOD 2009:80).

1.7.3.2 Planning the internal audit function's activities based on risk

The chief audit executive should base the priorities of the internal audit function's activities on risks identified during, *inter alia*, the risk management process (IIA 2009(a):25-26,93-94; IOD 2009:94).

1.7.3.3. Risk-based internal audit engagements

All internal audit engagements should be planned according to risks threatening the operations of the business process, unit or activity under investigation (IIA 2009(a):31-32,121-126; IOD 2009:15). This forms the basis for the rest of the study and is briefly introduced in this chapter.

1.7.4 Important sources on risk-based internal auditing

As discussed above, one of the areas where risk concepts can be incorporated into the internal audit function is in the performance of an internal audit engagement. This section briefly mentions some of the important sources that are available on the topic.

1.7.4.1 Institute of Internal Auditors Incorporated

The *Standards* states that the internal auditor should consider, *inter alia*, the following with reference to the planning of each internal audit engagement (IIA 2009(a):31):

- The significant risks to the activity under review... means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's risk management…
- The opportunities for making significant improvements to the activity's risk management…

This implies that the risks threatening the organisation's objectives should play a significant part when planning an internal audit engagement. But do internal auditors adhere to these mandatory requirements? According to the global CBOK study, 60% of respondents (full compliance) confirm that their adherence to the *Standards* includes planning of the internal audit function's activities for the year that is based on risk, with a possible 32% (partial compliance) that could also adhere to this guideline (IIA Research Foundation 2007:166). The assumption could therefore be made that the internal audit function's annual plan should be focusing on strategic high-risk areas (refer to section 1.7.3.2 on p. 35).

Although not mandatory guidance, the IIA issued various practice advisories that also refer, both directly and indirectly to risk-based internal auditing and will be discussed in the context of the study.

The CBOK study also indicates (IIA Research Foundation 2007:213) that 70.8% of respondents do follow a "structured and systematic" approach when performing the audit processes, including in the planning phase of the internal audit engagement. No clarity was provided on what the structured and systematic approach entails, but it was substantiated by the results of many global research studies (Ernst & Young, Institute de L'Audit Interne, IIA Belgium cited in IIA Research Foundation 2007:388,391,393). The study further identifies that 78% of respondents indicate that they use some form of a risk-based technique when

planning the internal audit engagement (IIA Research Foundation 2007:224). No specifications are provided on what is meant by a risk-based technique.

A recent study performed in Europe (Castanheira, Rodrigues & Craig 2010:95) on the use of a risk-based approach during the function's annual planning as well as during the audit process, provides more specific information. Although 82% of the respondents indicated that they perform a risk-based approach when drawing up the internal audit function's annual plan, only 31% is performing a comprehensive risk-based approach during the internal audit engagement planning. Other drivers include internal controls, processes (cyclical approach) and systems.

It is logical to conclude that the methodology used when performing an internal audit engagement will differ from one organisation to another. The question remains whether internal audit engagements are performed by focusing on the compliance of controls of high-risk areas, or whether all the risks threatening the objectives of the activity are included in the engagement.

1.7.4.2 Brief overview on literature

After a thorough search performed of the relevant literature and information resources such as libraries, the National Research Foundation (NRF), University Microfilm International (UMI), and the Internet in general, it could not be established whether a formal research study has been conducted on the use of a structured risk-based internal audit model with regard to internal audit engagements. Some of the studies performed (Sutton & Hampton 2003; Curtis & Turley 2006; Prinsloo 2008) do address the effect of risk on the external audit methodology and a study performed by Wheeler (2005) applies risk-based auditing in IT environments.

In Annexure A (on p. 451), a list and short discussion is provided of formal theses and dissertation studies conducted from 2000 to date obtained with regard to internal auditing, risk-based auditing, risk management and corporate governance that relate to this study.

The following databases were explored:

- UMI – dissertations;
- the SA NRF – current and completed theses and dissertations; and
- Networked Digital Library of Theses and Dissertations (NDLTD) – national and international theses and dissertations.

The IIA Inc. textbook (Reding, Sobel, Anderson, Head, Ramamoorti & Salamasick 2007:10/23-10/35) uses the COSO Report (2004) methodology in the planning phase of an assurance engagement. David Griffiths (2006(a); 2006(b)) has written two manuals, namely *Risk-based internal auditing: An introduction* as well as *Risk-based internal auditing: Three views on implementation on this matter*. This material is discussed more comprehensively in Chapter 4 of the study.

1.7.5 Conclusion

After the publication of *Internal control: Integrated framework* (COSO 1992), the internal audit environment agreed that the traditional way of performing internal audit engagements (being the watch dog) had to make way for a new paradigm (guide dog). Similarly, after the publication of *Enterprise Risk Management* (COSO 2004) and the implementation of the revised *Standards* (IIA 2006(a) and 2009(a)), the way internal auditors address risk will most probably have to change. It seems that this change has taken place with regard to the role of internal auditing in the risk management process (IIA Research Foundation 2007:212), as well as the incorporation of the outcome of the risk management process into the planning of the activities of the internal audit function (IIA Research Foundation 2007:205). It does however seem that, if the lack of literature on the subject is an indication, it has only slightly changed the way internal audit engagements are performed. This study, as discussed in the next section, focuses on addressing this gap by incorporating risk into the internal audit engagement methodology.

1.8 PROBLEM STATEMENT AND RESEARCH METHODOLOGY

This section provides an exposition of the research methodology that is followed in the study. It includes the research problem, objectives, scope and limitation, and the various literature and empirical research studies performed.

1.8.1 Research problem

The business environment is changing and becoming more complex. The internal audit profession, true to their definition of adding value, has to keep up with these changes. As was discussed throughout this chapter, various factors contribute to the necessity for internal auditors to perform their tasks more effectively and efficiently.

In SA, an internal audit function and a proper established risk management process are both seen by the private sector (IOD 2002, 2009) as well as the public sector (SA – PFMA 1999; IOD 2002; SA – MFMA 2003) as necessities for sound corporate governance. The IIA, as the governing body of the profession, has not only included risk management into their formal definition of internal auditing (IIA 2009(a):2), but has also developed materials on guiding its members on the role internal auditing should play regarding the risk management process (IIA 2004; IIA 2009(a):107-110).

This is, however, not applicable for guidance on risk-based internal auditing. Very little formal IIA Inc. guidelines as per the IPPF were found on the IIA Inc. website on performing a risk-based internal audit engagement.

The research problem is thus the following:

- Various factors, for example, the changing internal audit environment and changes within corporate governance guidance, underline the necessity for internal auditors to perform internal audit engagements more effectively and efficiently (refer to sections 1.2 on p. 4, 1.3 on p. 12 and 1.4 on p. 20).

- Internal audit methodology has changed over the last few decades, but more change is needed to address risks (refer to sections 1.6 on p. 29 and 1.7 on p. 32).
- The IIA has not provided their members with methodology, guidelines or a tool on how to perform an internal audit engagement more effectively and efficiently based on risk (refer to section 1.7.4 on p. 35).

1.8.2 Research objective

The main objective for this study is to develop a risk-based internal audit model that can be used by internal auditors when planning internal audit engagements. Note that this model does not include the internal auditor's responsibilities when fraud or other irregularities are discovered and that the professional judgement of the internal auditor must not be underestimated. This study aims at a model that will assist in securing that:

- areas with high operational risks are included in the planning of the internal audit engagement;
- areas with low risks are only included for the sake of a surprise investigation; and
- areas where risks remain high after controls are implemented are not investigated in detail, but rather reported to management on a timely basis.

Thus, the model will assist the internal auditor to focus on the areas that need attention and not waste time on areas that are insignificant. The effect is that scarce internal audit resources can be allocated to areas where they will add the most value to the organisation.

As the fieldwork that is performed during the execution of an internal audit engagement is determined by the engagement work programme with its list of engagement procedures, the development of the model focuses on the planning phase of an internal audit engagement, specifically the development of the engagement work programme. This will result in the following sub-objectives:

- High-risk auditable areas should be included in the planning of the audit engagement (engagement procedures included in the engagement work programme).
- Internal auditors should not waste scarce resources on auditing low-risk areas (engagement procedures not included in the engagement work programme).
- High-risk areas that remain high-risk after appropriate controls have been implemented should be reported to management on a timely basis (not included in the engagement work programme, but a finding in the engagement report – either on an interim basis or included in the final report).

1.8.3 Scope and limitations

Internal auditing is a global profession and much literature with discussions on risk-related topics exists. The study investigated as much of this literature as possible and obtained thorough background information in preparing for the development of the risk-based internal audit model. This study limited its scope by attempting to obtain all the most relevant information on the topic, obtaining input from SA chief audit executives, and testing the model in a SA context.

Although the core objectives of the private and the public sectors differ, the incorporation of internal audit methodology, and more specifically risk-based internal auditing, is the same for both these sectors. Therefore, the study includes both the private and the public sectors (refer to section 1.5 on p. 24 for a detailed discussion).

Lastly, it should be noted that one of the key pre-requisites for the use of this model by the internal audit function is that the organisation should be mature in their approach to risk management (refer to section 3.6 on p. 205 for an explanation of the term ‘risk maturity’). Thus, only risk mature organisations are included in the study.

1.8.4 Research methodology

According to researchers (Leedy & Ormrod 2005:2; Saunders, Lewis & Thornhill 2007:2-3), research is the systematic and logical process of collecting, analysing and interpreting information obtained through previous studies (literature review), or by obtaining new data (empirical review), with the objective of understanding the specific field that is studied. This study comprises both these research methods. In the first instance a literature review was performed to assist in understanding fundamental principles within the internal audit environment, external factors influencing the methodology of the internal audit profession, as well as risk and related methodology. Thereafter, empirical research methodology was used to obtain new evidence on the topic and test the theoretical framework drawn up after studying the relevant literature.

1.8.4.1 Literature review

A literature study has as its main objective the investigation of theoretical perspectives and previous research findings that are relevant to the current study and that will guide the researcher with the empirical study (Higson-Smith 2000:29; Leedy & Ormrod 2005:64; Saunders *et al*. 2007:595; Wikipedia n.d.(a)). According to Saunders *et al.* (2007:54), two of the most important characteristics of a literature study are that it should be comprehensive and critical. Mouton (2001:90-91) adds to this list by arguing that it should be topical and not navigated by date, and that it should be well organised and thus easy for the reader to understand the flow of information and ideas.

The benefits of performing a literature review include (Higson-Smith 2000:29-31; Mouton 2001:87; Leedy & Ormrod 2005:64-65; Saunders *et al.* 2007:57-58):

- providing of new ideas, perspectives and approaches to the problem;
- refining the research problem and objectives;
- discovering insight into other research approaches;
- obtaining current opinions and trends on the topic;

- eliminating duplication on research already performed;
- identifying other potential research possibilities;
- providing other relevant sources, measurement tools and methodologies; and
- assisting with interpreting research findings.

The objective of this literature study was to develop a preliminary risk-based internal audit model that will assist internal auditors while performing an internal audit engagement on a specific operational area. This model will force the internal auditor to focus on the high risks threatening the reaching of the objectives of the area under review. The output of the risk management process that was performed by management on the operational area is used as a basis to determine what should be included in the scope of the risk-based internal audit engagement with the specific aim of ensuring the following:

- High-risk areas are included in the planning phase of the engagement.
- High-risk areas where management has not been able to mitigate the risk within acceptable levels are not investigated in detail, but will be brought to management's attention for further action. Only areas where the internal auditor can add value are investigated as part of the audit engagement. Thus, valuable time is not wasted.
- Low risks are not included in the planning of the engagement, but are limited to surprise checks only.
- The inherent risk (susceptibility of an item to risk) and residual risk (the remaining risk after controls have been put into place) of all operations are obtained from management.
- The differences between the inherent and the residual risks are used to determine high-risk areas, low-risk areas and the mitigation of the risks by management.

This concept will be explained further and discussed in detail in section 4.5.5 on p. 274.

With the above in mind, the result of the literature review is documented in Chapters 2 to 4, and provides the basis for this study's empirical studies.

1.8.4.2 Empirical studies

Empirical research is a study that is based on direct or indirect experimentations, surveys, case studies, or observations to obtain an answer on a specific research question (Mouton 2001:144; Saunders *et al*. 2007:132-134; Wikipedia n.d.(a)). This type of research can comprise many research methods or designs (Mouton 2001:144; Tustin, Lighthelm, Martins & Van Wyk 2005:115-328; Leedy & Ormrod 2005:87-88; Saunders *et al.* 2007:608) that can be divided into three main groups, namely qualitative, descriptive and experimental. A common factor in all three these methods is that data is gathered – primary data (new data), existing data, quantitative data (numerical data) and/or qualitative data (non-numerical data). This study comprised multiple empirical research methods (as discussed in sections 1.8.4.2.1 to 1.8.4.2.3) incorporating various types of data.

1.8.4.2.1 Risk maturity

- **Objective**

The first empirical investigation was performed to determine the true status of the implementation of an effective risk management strategy (also referred to as the level of risk maturity) within specific organisations. The objective was to identify organisations that are risk mature as this is one of the pre-requisites for an internal audit function to be able to use the risk-based internal audit model.

- **Methodology followed**

The research methodology that was used to determine the level of risk maturity of the organisations was a qualitative method, namely *evaluation research: implementation evaluation* (Mouton 2001:144,158-159) that has as its main objective to determine whether a programme, policy or strategy has been

properly implemented as planned or developed. Mouton (2001:159) concludes that when using this type of research, the evaluation could be, *inter alia*, theory-based (tick the 'black box'). The analysing of existing documentary sources is also commonly used. The data analysis is qualitative in nature and the control over the research context by the researcher is low. This empirical study was conducted in three parts as explained below.

For part one, a pre-developed model of the Risk and Insurance Management Society Inc., or RIMS (2006), was used to measure the risk maturity of the organisations. After a thorough search, it was decided that this model is the most commonly used based on the references made to this document by various risk experts and risk-related organisations (Lenckus 2006; McDonald 2007; Liebowitz 2007; De la Rosa 2008(b)). This model is also based (Liebowitz 2007:44) on the capability maturity model developed by the Software Engineering Institute (2010) of the Carnegie Mellon University in the USA in the late 1980s to early 1990s that is widely used and recognised by various professions (Hillson 1997:36; Liebowitz 2007:44; McDonald 2007:29; Chapman 2009). Although a few other risk models were identified, they were either older than the RIMS model, not commonly used, or for a specific target group, for example, the defence force or transportation and logistics (refer to table 3.5 on p. 209) As mentioned in section 1.7.3 on p. 34, the concept of risk maturity and the use of a model to measure the maturity of a specific organisation are discussed in great depth in Chapter 3. For the purpose of introducing the risk maturity model as part of the research methodology, the model is only briefly discussed in this chapter.

RIMS (2006), a non-profit organisation that serves about 9600 risk management professionals globally, has developed a risk maturity model. The model was developed after extensive research was done by studying case studies from the last twenty-five years. The risk maturity model has advantages for various stakeholders, including practitioners, the risk management-responsible individuals, organisations and management. However, the model's main objective is to highlight aspects of an effective risk management framework and assist stakeholders in achieving this goal. The model consists of six criteria or attributes, five steps or phases for each criteria and a deliverable matrix for each criteria

(refer to Annexure B to E on pp. 459 to 466 for a detailed discussion of each of these).

The six criteria are:

- culture;
- involvement in strategy setting;
- risk management policy setting;
- risk management process;
- people; and
- risk management performance.

For the purpose of this study, each of the thirty areas (six criteria X five steps) equals five points, totalling a maximum of hundred and fifty points.

The RIMS model was used as a basis for the list of deliverables against which to measure the participating organisation's risk maturity (refer to Annexure F on p. 474 for the final scorecard used in this study). For the purpose of evaluating the deliverables against sound corporate governance risk management requirements for SA private sector and public sector organisations, the scorecard was adapted after taking into account documents such as the second King Report on Governance (IOD 2002) – note that King II was used as King III was only available in draft format when the scorecard was developed.

In the second part, the organisations' financial statements, information on the Internet and other relevant information with regard to risk management of the organisations were gathered.

Thirdly, each organisation's information was compared to the final list of deliverables per criteria and the outcome was documented on the scorecard (refer to Annexure G on p. 477 and H on p. 479 for the results of the participating organisations).

For the purpose of this study, all organisations with a risk maturity score of a hundred or more were classified as risk mature. The reason for this minimum is

that an organisation that was not at least on step three was not suitable to be incorporated into this study (refer to Annexure B to E on pp. 459 to 466 for the detailed criteria and deliverables for each step).

The above is explained by means of the following hypothesis example:

Organisation X has the following risk management principles in place as measured by the deliverables for each of the following criteria:

	Criteria / Attributes	**Step/Phase (max = 5)**	**Score (step x 5)**
1	Culture	4	20
2	Strategy setting	3	15
3	Risk management policy	3	15
4	Risk management process	3	15
5	People	2	10
6	Risk management performance	2	10
	TOTAL		**85**

Organisation X is thus not classified as a risk mature organisation for the purpose of this study (score is less than a hundred points).

- **Sample**

For the private sector (refer to section 1.5 on p. 24) the top forty companies listed on the JSE Limited as at 8 April 2009 were used as the sample. The reason being that all companies listed on the JSE Limited have to comply with the King Report on Corporate Governance requirements since 1 September 2003 (Baue 2003) enhancing the likelihood of a higher risk maturity. Additionally, the sample choice was influenced by the researcher's professional judgement. The preliminary literature review already identified studies that indicate that not all organisations listed on the JSE Limited adhere to the King Report requirements (Business Times n.d.; Faure & De Villiers 2004:67-69). It could, however, be argued that the top forty listed companies would probably have to adhere to these requirements to be able to stay at the forefront of their respective markets. Furthermore, the TOP 40 Index represented 87.64% of the total market value of

the JSE's All Share Index on 27 February 2008 (Marx 2008:346) and R3 milliard market capital on 8 April 2009 (Mathephe 2009), thus not only representing the largest companies, but also a wide spectrum of stakeholders. Lastly, thirty-two of these companies' internal audit functions are members of the IIA (SA) with a further two fully outsourced to a well-known internal audit consulting group, namely Aurco (Erasmus 2009). The McGregor BFA Index (Mathephe 2009) is used to determine the top forty companies – refer to Annexure G on p. 477 for a list of the companies.

For the public sector (refer to section 1.5 on p. 24), the thirty-seven national government departments were included in the sample – refer to Annexure H on p. 479 for a list of the departments. The reason was that according to the Auditor General (AGSA 2009(a):1,12-17; AGSA 2009(b):5), this is the group with the most unqualified audit reports (21%) compared to provincial government organisations (6%) and local authorities (2.8%). These statistics suggest that these departments would most probably have a better chance of adhering to rules and regulations, including the establishment of a risk management framework. Secondly, according to a status report on risk management for provincial government (SA – Public Service Commission 2002), three of the nine provinces do not comply with risk management strategies according to the PFMA. This could also be interpreted as provincial departments possibly having a low risk maturity level; as such, these departments are not included in the sample.

1.8.4.2.2 Risk-based internal audit model

- **Objective**

The second empirical research study's objective was to refine the risk-based internal audit model that was developed after studying the literature.

- **Methodology followed**

Formal interviews were conducted with the chief audit executives of both the private and the public sectors in the internal audit function, using a structured questionnaire as a platform.

The questionnaire was set by obtaining information during the literature review and focused on the following:

- Determine the relevance and importance of risk management for the organisation and more specifically the internal audit function.
- Determine whether the internal audit function incorporates risk concepts into its activities, for example, auditing the risk management framework and/or process and performing a risk assessment when planning the activities of the internal audit function.
- Determine whether the internal audit function incorporates risk-based planning into their internal audit engagements.
- Obtain input into the preliminary developed risk-based internal audit model and adapt the model accordingly.

Although a formal questionnaire was developed, the method that was used to gather the desired information was a *descriptive method: survey research*, obtaining quantitative primary data (Mouton 2001:152-153). This data is collected by means of, *inter alia*, personal interviews and the data consist of facts, opinions, beliefs, attitudes or behaviour (Zikmund 2000:190; Mouton 2001:152-153; Tustin *et al.* 2005:145; Saunders *et al*. 2007:310). This method was chosen for various reasons. Firstly, risk-based internal auditing for internal audit engagements is a fairly new concept, as can be seen from the recent studies performed in the internal audit field incorporated into the CBOK publication (IIA Research Foundation 2007:359-405). Secondly, although organisations may believe that they are performing risk-based internal audits, it is possible that their internal audit engagements still focus on compliance of controls with a stronger focus on risk, instead of a formal risk-based approach.

After consulting with internal audit researchers (Du Bruyn 2008; Fourie 2008; Barac 2008; De Jager 2008) and practitioners (Du Plessis 2008; De la Rosa 2008(a); Lubbe 2008(b)) on the research methodology that should be used to develop the model, it was agreed that a structured interview would most probably deliver the best results. It was felt that the preliminary risk-based internal audit model, being a difficult concept to explain, would run the risk of being misunderstood if presented *via* a questionnaire, and that valuable input could also be lost. As such the model was explained to the researchers and practitioners during an interview.

Lastly, as the internal audit profession is in a growth phase, the IIA (SA) is overwhelmed with requests to circulate formal research questionnaires. Veronica du Preez (2008), chief executive officer of the IIA (SA) has confirmed this fact and agrees that it is becoming more difficult to get the cooperation of internal auditors to complete questionnaires.

- **Populations and sample**

The population consisted of all risk mature organisations as identified after the previous empirical study was performed (refer to section 1.8.4.2.1 on p. 44). For the purpose of this study the objective was to use only risk mature organisations. The sample was drawn from the population and included:

  - all the organisations with a risk maturity score of a hundred points or more (refer to section 1.8.4.2.1 on p. 44);
  - a maximum of five private sector and five public sector organisations was included in the sample. The five organisations from each sector with the highest risk maturity score were selected. The reason for the sample size was that input from the chief audit executives was needed to refine the model and less than ten views could have resulted in not obtaining a variety of views. However, after the ten interviews were performed, should the researcher be of the opinion that more views needed to be obtained, the sample may be increased;

- if there were not ten organisations with a risk maturity score of a hundred points or more, the five public sector and five private sector organisations with the highest scores would be chosen; and
- if a specific sector had a very low score for all its organisations included in the population, this sector was treated differently. Chief audit executives were not questioned to refine the risk-based audit model, but to try and get an understanding as to the reasons why they are not risk mature and how it affects the internal audit function's activities. This could result in a second questionnaire being set and sent out.

1.8.4.2.3 Testing the model (case study)

- **Objective**

The third empirical research study was conducted to test the risk-based model to determine whether it could be used in practice, and if so, whether there is an improvement in the internal audit engagement. Possible improvements are measured by:

- performing less engagement procedures but including all the high-risk areas;
- identifying all (and even more) of the significant findings; and
- reporting significant findings on a more timely basis.

It was anticipated that the results of this empirical study could probably also be used to refine the risk-based internal audit model even further.

- **Methodology followed**

The methodology used was *ethnographic: case study* and was qualitative in nature (Mouton 2001:149-150; Yin 2003:1). According to Yin (2003:2-4) a case study approach allows the researcher to gain an understanding of the holistic and unique characteristics of a given real live event.

The planning phase of an internal audit engagement that was previously performed by the sample unit's internal audit function was re-evaluated using the risk-based internal audit model. The internal audit engagement planning, more specifically the engagement work programme, with its detailed engagement procedures, was re-performed. The original engagement work programme and detailed engagement procedures were compared with the ones drawn up using the risk-based internal audit model. Possible differences, advantages, disadvantages, improvements and weaknesses were identified. These were then used to refine the risk-based internal audit model further.

- **Population and sample**

The population was the ten organisations with the highest risk maturity score as determined under section 1.8.4.2.1 on p. 44. One organisation in each of the private and the public sectors was chosen to be in the sample unit. The one organisation in each sector with the highest risk maturity scores was considered first. The input received from the interviewees during the interviews performed (refer to section 1.8.4.2.2 on p. 48), for example, the willingness to participate, was considered. Lastly, professional judgement was also used when choosing the two organisations. When choosing the internal audit engagements, the criteria varied from the engagement being performed on a high strategic risk area, to being an assurance engagement as appose to being a consulting engagement. This case study research methodology is supported by Yin (2003:39-46) who confirms that a single case study can be used when a theory is being tested. In this case the existing theory was tested against the newly developed risk-based internal audit model.

1.8.5 Conclusion

The research methodology was developed in such a manner that a solution for the research problem, namely to provide internal auditors with a tool in the form of a risk-based internal audit model that will assist them in performing the planning phase of internal audit engagements more effectively and efficiently, could be achieved.

The study aimed to first develop a preliminary model by obtaining sufficient information using a literature review (Chapters 2 to 4). Thereafter, primary data was collected to improve the model, the model was tested in a practical scenario, and the model was then refined into a useable tool for internal auditors (Chapter 5).

1.9 LAYOUT OF THE STUDY

The study comprises 6 chapters, consisting of the following:

Chapter 1 – Introduction and background to the study
The first chapter investigates background information relevant to the study, identifies a research problem as a result of the information obtained, and formulates a research objective and methodology to be followed.

Chapter 2 – The evolution of the internal audit profession
In this chapter the changing role of the internal audit profession is discussed and benchmarked against the value that it should add in the areas of risk management, control and governance processes.

Chapter 3 – The development of corporate governance with specific reference to risk management
This chapter deals with the development of corporate governance, and more specifically risk management as one of its cornerstones. It explores the concept of risk, risk management, the accountability theory and responsibilities of various role players with regard to risk management, the risk maturity of an organisation and how this will affect various role players, as well as the future of risk management.

Chapter 4 – The role of internal auditing with specific reference to risk
In Chapter 4 the responsibilities of the internal audit function with regard to risk are investigated. The chapter concludes with how internal audit engagements can be improved to adhere to these responsibilities, including the development of a risk-based internal audit engagement model. Current and future trends with

regard to internal auditing and risk management are studied to determine possible deficiencies, gaps, best practices and expectations.

Chapter 5 – Research results of the empirical studies: risk maturity, refining the risk-based internal audit engagement model and testing the model

In this chapter, the results of the three empirical studies are provided and discussed. Risk mature organisations are identified by using a risk maturity model. The preliminary risk-based internal audit model is refined by developing a questionnaire and performing structured interviews with chief audit executives of risk mature organisations. Lastly the risk-based internal audit model is tested by comparing the engagement planning of an audit engagement previously performed by two (one in each of the private and the public sectors) of the risk mature organisations. The engagement planning is re-performed using the risk-based internal audit model. Differences are investigated and the risk-based internal audit model is further refined.

Chapter 6 – Recommendations and conclusions

Based on the final findings, recommendations are provided on the use of the model by various organisations. Further research is identified and final conclusions are made.

1.10 CONCLUSION

This chapter consists of two interrelated parts, first introducing the need for the study, and secondly, explaining the research methodology followed in the rest of the chapters.

The introduction of the study first debates the changing internal audit environment with specific reference to:

- the governing body of the profession, namely the IIA, being structured in such a manner that internal auditing is globally competitive yet locally relevant;

- the growth in the IIA membership not necessarily meeting the needs of all stakeholders;
- the scarcity of competent internal auditors; and
- guidance issued by the IIA relevant to corporate governance and risk management.

Thereafter, the influence of the development of corporate governance, globally and in SA, with specific focus on corporate governance codes and legislation, as well as corporate scandals, on the internal audit profession is briefly discussed.

Another benefit to having more effective and efficient approaches to internal audit engagements is the external auditor making use of the work of the internal auditor. Although numerous similarities and differences exist between the external audit and internal audit professions, both these parties recognise that they could benefit from working together. Guidance on how to improve coordination, as well as what is expected from the internal auditors for external auditors to be able to rely on their work, is briefly discussed.

Both the private and the public sectors are included in the study. The reason is that although there are many differences, for this study, the similarities are more relevant and are briefly discussed.

Change in the business environment is a constant. Internal auditors, as the right hand of management and assurance providers to the board of directors, need to adapt to these changes. This is also relevant to the internal audit methodologies and the way internal audit engagements are performed. One way of adopting new internal audit methodologies is the incorporation of risk into the performance of internal audit engagements. Limited IIA guidance exists on this topic. Practice Advisory 2210.A1-1 (IIA 2009(a):56) urges internal auditors to conduct a risk assessment as part of their planning strategy when performing an internal audit engagement. In April 2010, the IIA Inc. issued a further Practice Advisory 2200-2 (IIA 2010) addressing the fact that internal auditors should only audit key controls that mitigate risks that are significant to the organisation as a whole and not only

the activity under review. However, this guidance remains limited, as some of the crucial elements are not addressed in full. Furthermore, this study could complement the above-mentioned practice advisories by developing a tool that can provide additional guidance on how to implement a risk-based approach when performing an internal audit engagement (refer to section 1.2.4.1 on p. 9).

This study focuses on the development of a risk-based internal audit engagement model. The research methodology consisted of:

- a literature review to obtain an understanding of the fundamental principles of the internal audit environment, corporate governance, risk management, the role of internal auditing in risk-related aspects, and risk-based internal auditing;
- the development of a preliminary risk-based model for the planning phase of an internal audit engagement;
- three empirical studies, namely:
    - testing of organisations in both the private and the public sectors to determine the level of risk maturity;
    - obtaining of further evidence from chief audit executives of risk mature organisations to refine the risk-based internal audit model; and
    - testing the final model in a practical scenario, and if needed, adapting the model.

The following chapter is the first of three chapters covering the literature review, and focuses mainly on the evolution of the internal audit profession.

CHAPTER 2
THE EVOLUTION OF THE INTERNAL AUDIT PROFESSION

2.1 INTRODUCTION

Internal auditing is a relatively new discipline compared to most other business related disciplines, with practitioners active in both the private and public sectors worldwide (Dittenhofer 2001(a):458; Chapman 2004:42). It has evolved over a number of years, and when analysing various debates, it can be concluded that internal auditing is a profession (Dierks & Davis 1980:36-37; Sawyers *et al.* 1996:17-20; IIA 1999:33-36; Fogarty & Kalbers 2000:130-133; O'Regan 2001). The profession's evolutionary progress has reflected the ongoing change in both the methods and philosophy of conducting the affairs of organisations. Currently, the profession is at a crucial stage as a result of the rapidly changing environment in which internal auditors operate. They need to understand who they are, what is expected of them, and where they are going (Dittenhofer 2001(a):458; Nagy & Cenker 2002:131-32; Deloitte & IIA (UK and Ireland) 2003; PWC 2008(a):2).

In 1944, Arthur E Hald (cited in Flesher 1996:3), one of the founders of the IIA, made the following statement:

> Necessity created internal auditing and is making it an integral part of modern business. No large business can escape it. If they haven't got it now, they will have to have it sooner or later, and, if events keep developing as they do at present, they will have to have it sooner.

These words became true as internal auditing became one of the fastest growing professions of the second half of the twentieth century (Flesher 1996:3 – also refer to section 1.2.2 on p. 6 for a discussion on the growth of the profession). With this growth, management demanded more from the internal audit function. The activities of internal auditing expanded from performing assurance activities for management to assisting management with their responsibilities, thus making the responsibilities of modern internal auditing as broad as the current business environment.

With the turn of the century, the business environment noted that some dramatic changes were about to occur. Arnold Baker (cited in Marks 2001:44), chief economist of a large organisation in the USA, predicted that there was going to be a fundamental change in the global economy, unlike anything seen before. This brought about a need for internal auditors to adapt to this fast changing environment. The IIA, as the governing body of the profession, had to stay abreast of these times and, in 1999, new guidance was issued. One of these changes is the incorporation of risk methodology within the duties of the internal auditor, which is the concern of this study.

This changing role of internal auditors, with specific reference to risk, can only be fully appreciated if the evolution of the profession is properly understood. With this objective in mind, the rest of this chapter provides an overview of the history of auditing and the birth of the internal audit profession. The evolution of the profession is discussed and the changes within the profession examined as well as external factors affecting the profession, including the identification of possible threats to the profession, and lastly, determine what is meant by an effective and efficient internal audit function.

2.2 THE HISTORY OF AUDITING AND INTERNAL AUDITING

Internal auditing has developed from auditing (now more commonly referred to as external auditing). This section provides a brief overview of this evolution – the development of the internal audit profession and its governing body – both from a global perspective, as well as in terms of the developments in SA.

2.2.1 The history from a global perspective

The audit profession has developed over many years, with evidence of its existence dating back to 4000 BC, where businesses and governments in the Near East instituted the first formal record-keeping systems. In 3500 BC, records found of a Mesopotamian civilisation indicated tick marks, dots and check marks next to financial transactions. The Zhao Dynasty in China, as well as other developing communities of the time, had similar types of systems in use – all

developing a detailed system of checks and counterchecks (Brown cited in Ramamoorti 2003:3). With these developments the first system of verification was introduced.

The concept of auditing evolved further during the industrial revolution in England, and modern auditing was born. The need for an independent and reliable verification process to ensure that funds are utilised efficiently and that financial records are a true and fair reflection of the financial position and financial performance of an organisation, was the cornerstone of auditing. The process entailed that written records were scrutinised and entries in the accounting records were compared to the supporting documentation (Mautz & Sharaf 1961:158-161).

In the early 1900s, the concept of auditing evolved into two unique areas of specialisation, namely internal auditing and external auditing (Mautz cited in Ramamoorti 2003:3). External auditors performed the activities described in the previous paragraph. But economic growth had made it difficult for organisations to maintain control of their business activities and operational efficiency. Management had lost direct contact with most of its subordinates and needed some means of evaluating the efficiency of the work performed by its employees, and their honesty. To overcome the problem of controlling the activities of the organisation, people known as internal auditors were appointed to review and report on what was happening within the organisation; thus providing assurance to management that their policies, plans and procedures were performed as intended (Sawyers *et al*. 1996:9; Ramamoorti 2003:4; IIA n.d.(a)).

In these early years, as an internal business function, the internal audit function primarily focused on protection against payroll fraud, and the loss of cash and other assets. In subsequent years, the scope was extended to the verification of almost all financial transactions (Reeve 1986:34). The scope gradually evolved from an audit *for* management to ensure adherence to policies and procedures, to an audit *of* management approaches, for example, risk management. This is underlined by all the changes that have taken place in the profession during the

last decade (Hermanson & Rittenberg 2003:32; Chapman 2004:40-47; Spencer Pickett 2004(a):10-14; IIA n.d.(a)).

2.2.2 The evolving role of the Institute of Internal Auditors

As the profession evolved, internal auditors wanted greater recognition of their function and on 17 November 1941 the IIA Inc. was established in the USA (IIA n.d.(a)). The initial purpose of the IIA Inc. was to provide internal auditors with an opportunity to share their common interests and concerns (Sawyer *et al*. 1996:9). Today, the IIA Inc. is an international organisation that meets the needs of more than 160000 members worldwide, and is dedicated to the continuing professional development of individual internal auditors and the global internal audit profession (IIA 2008) – refer to section 1.2.1 on p. 5 for a discussion on the structure of the IIA. The activities and duties performed by the IIA Inc. in providing leadership for the global profession include (IIA n.d.(a)):

- advocating and promoting the value of the profession to organisations;
- providing educational and development opportunities;
- providing standards and other professional practice guidance;
- providing certification programmes;
- researching, disseminating, and promoting knowledge to practitioners and stakeholders;
- educating practitioners and others on best practices; and
- bringing together global members to share information and experiences.

For a long time, the environment that internal auditors operate in, namely internal audit departments or activities (hereafter refer to as internal audit functions), lacked guidance on their role and responsibility towards the organisation they served. According to Mautz and Sharaf (1961:11), internal auditing was a well-established and well-respected activity, but there was little indication that it was well defined or clearly directed. The Statement of Responsibilities of Internal Auditing was prepared by the IIA Inc.'s research committee and approved by the board of directors at its meeting on 15 July 1947. The purpose of the Statement

was to establish a set of guidelines that defined the proper role and responsibilities of the internal audit function within an organisation (Flesher 1996:34). The Statement has been regularly updated and, in June 1999, the IIA's board of directors voted and approved a new set of guidelines in the PPF (IIA 2006(a):2), headed by the current internal auditing definition. More recently (2009(a)) the IPPF has come into circulation as the newest internal auditing statement.

To make sure that internal auditors keep up with changes in their environments, the IIA Inc. developed a CBOK during 1972 (Sawyers *et al.* 1996:29). This has been regularly updated, and during 1999, the IIA's Research Foundation developed the CFIA to provide internal auditors with guidelines regarding their knowledge and the competencies needed to stay in touch with the changing business environment (McIntosh 1999:5). More recently, in 2007, a new CBOK was released (IIA Research Foundation 2007) and this document will be re-issued in 2010. The IIA Inc. also developed a new CFIA to keep up with the trends as indicated by the CBOK (IIA n.d.(f)). Where relevant to this study, the requirements or guidelines as set out in the IPPF, CBOK and CFIA are discussed.

Although the headquarters of the IIA is situated in Orlando, USA, the Institute serves members globally. The IIA has two hundred and forty nine chapters and affiliates in more than hundred and sixty countries (IIA 2008), all forming part of the international IIA network. One of these chapters is the IIA in SA, which is a national institute (IIA (SA) n.d.(a)), serving more than six thousand members (Erasmus 2008). It is administrated as an association incorporated as a non-profit organisation.

2.2.3 Developments in South Africa

The IIA (SA) is governed by a voluntary board of directors, which is constitutionally elected by its members. Thirteen regional governors and their supporting committees serve members voluntarily in the various provinces (IIA (SA) n.d.(a)).

The IIA (SA) chapter (Van Wyk & Hodson 1998:21) was established in 1964; the driving force behind its establishment was the local internal auditors employed by international companies. In 1983 the chapter was upgraded to a national institute. The profession continue to grow (refer to table 1.1 on p. 7 for statistics) and legislation and regulation such as the Public Entities Act in 1992 and the first King Report on Corporate Governance in 1994, respectively mandating and recommending the establishment of an effective internal audit function, contributed tremendously to its growth.

Today, the internal audit profession is one of the leading global professions. In a recently published IIA Inc. document on successes around the globe, the IIA (SA) has contributed significantly, with either mandatory, recognition or recommendation of internal auditing in the following areas (IIA n.d.(h)):

- All public sector organisations must have an internal audit function that adheres to the *Standards*.
- The JSE Limited requires all listed companies to align with the King Report that either requires an internal audit function, or an explanation in the annual report as to why such a function does not exist. The function must also comply with the *Standards*.
- The following bodies advise all their members working in an internal audit environment to conform to the *Standards*:
    - South African Institute of Chartered Accountants (SAICA);
    - Institute of Public Finance and Auditing;
    - Independent Regulatory Board for Auditors;
    - Auditor General;
    - Audit Committee Forum;
    - African Organisation of Supreme Audit Institutions;
    - Eastern and Southern African Association of Accountants Generals;
    - Association of Certified Fraud Examiners; and
    - Business Against Crime.

These factors all contribute to the growth of the profession in SA. The fact that the country has a strong corporate governance culture with the three King reports being recognised worldwide, as well as legislation supporting internal auditing, makes SA a force to be reckoned with. This is evident from the fact that numerous senior internal auditors serve on the international committees that advise the global counsel; which in its turn has two SA members.

2.2.4 Conclusion

The history of the profession, both globally and in SA, is an indication that it has established itself as one of the successes in the modern business world. Internal auditing is increasingly recognised by various parties as a necessity for organisations. Factors such as the increased awareness of corporate governance, the rise of corporate scandals, the global financial crisis, globalisation, and many others, provide an opportunity for internal auditors to demonstrate their real capabilities. It is of the utmost importance that these opportunities are utilised to the maximum, benefiting the promotion of the profession. Therefore, an effective and efficient internal audit function, that adds value to all stakeholders, is a necessity. The IIA, as the governing body, must provide internal auditors with the needed guidance to ensure that this is possible.

2.3 THEORY OF INTERNAL AUDITING

To understand the responsibilities of the internal auditor, it is firstly important to determine the root theory that the profession is built on. The internal audit profession developed from the external audit profession (refer to section 2.2.1 on p. 58 for a discussion on the history of auditing) and it is therefore important to first understand the core role of the external auditor. The next section discusses the comparison of the two professions, followed by an explanation of some of the theory of external auditing, and how this relates to internal auditing.

2.3.1 Comparison of internal and external auditing

Before the theory of the two professions can be studied, it is important to understand some of the differences as well as tangencies of the two professions.

The first major difference is the employer of the internal auditor and the external auditor. External auditors are independently appointed by the shareholders (or owners) of an organisation (SA – Corporate Laws Amendment Act 2007:S90). They report to the shareholders as to whether the financial statements are prepared in accordance with an applicable financial reporting framework (SAICA 2009/10:ISA200-2), thus providing reasonable assurance that what is reflected in the financial statements is a true and fair view in accordance with the financial reporting framework. It should be noted that independence is of a crucial nature to external auditing. If the external auditor is not objective in the performance of his/her duties, the financial statements could reflect the wrong information to the shareholders and other users of the financial statements. Internal auditors are employed by management and have as their main objective to assist management with reaching the organisation's objectives (IIA 2009(a):15). Although the *Standards* urges that the internal audit function should be independent from management (IIA 2009(a):16), the question remains whether the internal audit function is truly independent as this will play a vital role when the external auditors must decide whether they will rely on the work performed by the internal audit function or not.

A second major differences lies within the objectives of the two professions. The external auditors' main objective is to provide assurance to stakeholders on the fairness of the financial statements (SAICA 2009/10:ISA200-3). The internal auditors, true to the definition of internal auditing (IIA 2009(a):2), must assist management in any possible way needed to achieve the organisation's objectives. This leads to a third major difference, namely the scope of activities.

The external auditor performs primarily financial audits, thus investigating transactions and balances to be able to adhere to the above objective. With regard to internal controls implemented by management, only those relevant to

the audit will be investigated. The depth of understanding of these controls will also be limited to that deemed necessary, thus minimising mistakes and fraud within the scope of the financial audit (SAICA 2009/10:ISA315-16). On the other hand, the only limitation on the scope of work performed by the internal audit function is what the board stipulates in the internal audit charter (IIA 2009(a):15).

Some of the most important areas where the two professions have tangencies include that both professions' activities involve testing by performing audit procedures. Although the main objective differs, both professions are involved with the organisation's system of internal control as well as being concerned with fraud and other irregularities. It is also true that both are based in a professional discipline that answers to standards and an ethical code. Furthermore, both have comprehensive communication and reporting duties to various parties.

A comparison between the two professions reveals further differences and similarities that are listed in table 2.1 on p. 66 (Sawyers, Dittenhofer & Scheiner 2003:7; Spencer Pickett 2003:74-80; Coetzee, Du Bruyn & Plant 2007:73; Balkaran 2008:22-23; Anonymous n.d.).

From the above discussion it is clear that although there are many differences and similarities between the two professions, there are enough points of contact between the two that they have an influence on one another. The next section discusses two of the principles of the ground theory of external auditing, namely the accountability and agency theories, and how these correlate with the internal audit profession.

Table 2.1: Comparison between internal auditing and external auditing (financial statement audit) in a South African context

Area	Internal Auditing	External Auditing
Qualifications and practical training	• No formal qualifications required • Could register as a CIA • For CIA designation 2 years practical training	• Registered Chartered Accountant (SA) • For CA(SA) 3 years practical training
Legislation/ regulations require organisation to appoint	Limited legislation, namely: • Public sector (PFMA & MFMA) • King Report III for all organisations	• Required by law (Corporate Laws Amendment Act 47/2007) for all private and public companies • Public Audit Act (25/2004) for all public sector organisations
Focus areas of main activities	• Past, present and future • No limitation on scope	• For financial statement audits focus mainly on historical information • No limitation on scope
Reporting scope	• Only internal • Comprehensive and only few guidelines on structure	• Internal and external • More structured reporting format
Timing of audit engagements	• Continuous	• Focuses mainly on year-end
Internal control	• Comprehensive assurance on the use of internal control mechanisms • Provide improvements if not efficient and effective • Could be involved with the implementations (consulting)	• Control mechanism only tested if it could have an effect on the financial statement audit (risks of material misstatements at assertion level) • Could provide advise on improvements
Improvement of the organisation's operations	• Perform comprehensive value-for-money investigations to identify areas of improvement	• Performance auditing for public sector by Auditor General • Communicate possible improvements identified during financial audit as part of internal communication

(Source: refer to discussion)

2.3.2 External auditing and the agency and accountability theories

Philosophers (Mautz & Sharaf 1961:158; Flint 1988:14-15) have come to the conclusion that auditing is a social phenomenon that merely exists because certain groups in society seek information or reassurance about the conduct or performance of others. The external audit process has, as its main objective, to report to the shareholders (other third parties may also use the information) its opinion as to whether the financial statements give a true and fair view of the organisation in accordance with an acceptable financial reporting framework for a specific period (SAICA 2009/10:ISA200-2). This principle is based on, *inter alia*, the agency and accountability theories. These theories, as well as their context within the internal audit environment, are briefly discussed.

The owner of resources/shareholders (principal) appoints managers (agents) who are charged with the responsibility to manage the resources on behalf of the principal (Sherer & Kent 1983:1; Watts & Zimmerman 1986:180-186; Dunn 1996:3-5). This is referred to as the agency theory. The agents have certain responsibilities, are accountable or answerable on how resources are spent, and should give account of their activities to the principal – also known as the accountability theory (Sherer & Kent 1983:1-3; Flint 1988:12-14; Loots 1989:2-4). In common language, accountability is referred to as the reporting process that takes place after an action(s) or decision(s) was implemented (Oxford Dictionary 2005:7; Wikipedia n.d.(c)). More scientific sources (Sherer & Kent 1983:1; Flint 1988:14; Du Toit *et al.* 2002:219; Pauw *et al.* 2002:26-27) describe accountability as officials and organisations being answerable for their plans, actions and outcomes to a broad scope of stakeholders.

The external audit profession is the independent link between the principal and the agent. The problem arises that the principal cannot normally verify the reasonableness of the information provided by the agent. To overcome this obstacle, independent external auditors are appointed to perform this task on behalf of the principal. All activities of the organisation feed into the accounting system. The external auditor verifies the reasonableness of the activities of the

organisation as reflected in the financial statements and reports to the principal on the fairness of the representation.

2.3.3 Internal auditing and the agency and accountability theories

With the evolution of the internal audit profession, the question arises whether the agency and the accountability theories can also be linked to it. Although, in theory, the process in place, as discussed in section 2.3.2 on p. 67, should be sufficient to satisfy the principal that all possible was done to optimise his/her investment, in practice there are many obstacles and gaps that could prevent an individual in reaching such a conclusion (Spencer Pickett 2003:24-25). These will not be discussed as this falls outside the scope of this study. However, a specific area where the internal auditor can play a significant part is in determining whether the operations of the organisation have been conducted in the most efficient and effective manner possible. Thus, although the external auditor will provide the principal with the assurance that the financial statements of the organisation are a reasonably fair reflection of the operational activities (SAICA 2009/10:ISA700-11), they cannot provide insight into the cost-efficiency and effectiveness of the operations.

Secondly, with the growth and increasing complexity of the modern business environment, it is impossible for management, as the agent, to be available at all places. They have to use other resources to assist them with ensuring that their rules, regulations, policies and procedures are adhered to by employees, and also in assessing if the measures that they have implemented are still relevant and sufficient to reach the objectives and goals that they have set. As schematically presented in figure 2.1 on p. 69, the internal auditor may assist in bonding the agent and the principal.

Thirdly, internal auditing, although appointed by management, employed by the organisation and administratively reporting to the chief executive officer, should report operationally or functionally to the audit committee (IIA 2006(a):41-44; Marx 2008:291; IOD 2009:97). This implies that all crucial findings discovered during the performance of internal audit engagements are brought to the audit

committee's attention. An effective audit committee must be independent (SA – PFMA 1999:S77; IOD 2002:186; KPMG 2005:26-32) with the majority of the members being independent non-executive directors. This implies that the audit committee is, *inter alia*, for the benefit of external stakeholders, including the principle. According to a study performed by Marx (2008:363), this is true for the private sector with 81.9% of audit committee members being independent and non-executive. A study performed by Van der Nest on audit committees in the public service in SA (2006:190-191) indicates that the public sector also adhere to their independent guidelines as stipulated in the PFMA (SA – 1999:S77), with 83% of participating departments appointing at least 60% of their members from outside the organisation. This is, however, not always the case for the public sector in other countries. A study performed by the IIA and KPMG in New Zealand (2009) on audit committees in the public sector showed only 11% have a majority of external members, thus jeopardising the audit committees' independence.

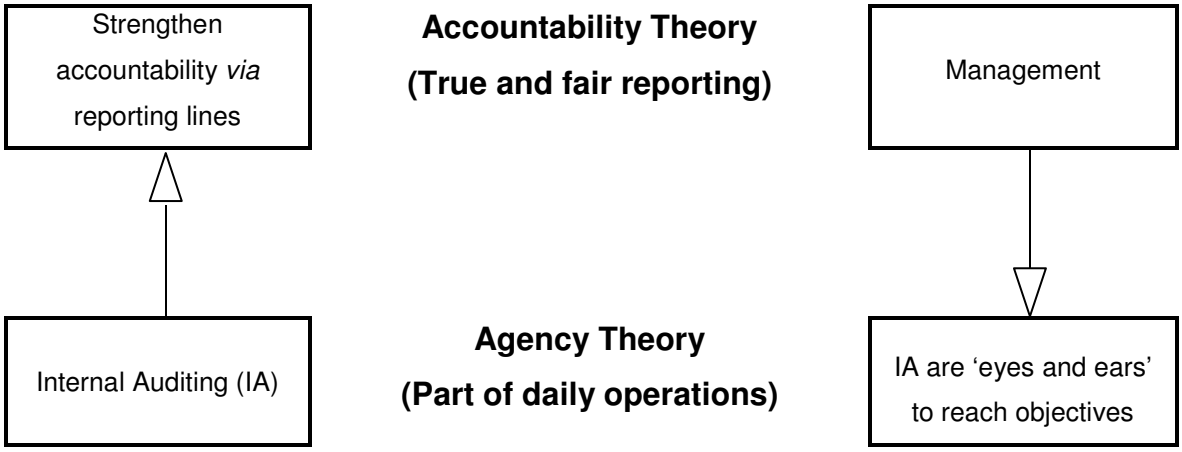


Figure 2.1: Internal auditing and the agency and accountability theories

The above figure 2.1 schematically summarises the discussion. The internal audit function are placed within the daily activities and operations of the organisation (assists with the agency theory specifically with regard to cost-effectiveness), but with direct reporting lines to the independent audit committee that, in theory, represents the principal (accountability theory). Management, however, uses the internal audit function to ensure that their reporting to the principal is fair (accountability theory) and uses internal auditing, as the right hand of

management, to assist the organisation in accomplishing its objectives (agency theory). This, according to the definition of internal auditing, includes the evaluation and improvement of risk management, control and governance processes.

2.3.4 Conclusion

Although it seems that literature is limited on the root theory of the internal audit profession, by using the external audit profession's theory as a basis, it is fair to conclude that internal auditors play an important role in assisting both the principal (shareholders) and the agent (management) in reaching their respective objectives. When investigating the recent changes within the profession, this statement is further strengthened.

2.4 CHANGES WITHIN THE INTERNAL AUDIT POFESSION

Many factors have contributed to the need for change within the internal audit profession (refer to sections 1.2 on p. 4 and 1.3 on p. 12 for a brief discussion). The IIA addressed this need by dramatically changing the definition of internal auditing. Other areas that have seen changes within the profession include, *inter alia*, the increase of outsourcing of the internal audit function, the requiring of new specialisation fields, and ultimately the IIA addressing this by issuing new guidance.

2.4.1 Definition of internal auditing

In 1999, after a long debate and numerous governing bodies investigating the trends in the modern internal audit profession, the IIA's board of directors approved a new definition to encompass all the changes within the profession (IIA 2009(a):2):

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve

the effectiveness of risk management, control and governance processes.

The definition of internal auditing, being the cornerstone of the profession, is the ideal means to explain the evolution of the profession and its modern trends. In table 2.2 on below, the key elements of the current definition are compared to those of the previous definition to emphasise the changes made in the profession.

Table 2.2: Comparison of the previous and current definitions of internal auditing

Previous definition	Current definition
Independent appraisal function	Objective assurance and consulting activity
Established within an organisation	Independently managed within an organisation
Examines and evaluates its activities as a service to the organisation	Adds value to improve the operations of the organisation
Assists members of the organisation in the effective discharge of their responsibilities	Assists an organisation in accomplishing its objectives
Does analyses, appraisals; makes recommendations; provides information concerning the activities reviewed	Uses a systematic and disciplined approach
Promotes effective control at reasonable cost	Evaluates/improves the effectiveness of the organisation's risk management, control and governance processes

(Source: IIA 1999:6)

The most important changes, as highlighted by the comparison in table 2.2 above, are discussed below.

2.4.1.1 Consulting activity

The consulting role of an internal auditor is added in the current definition. This role refers, *inter alia*, to providing assistance to management in accomplishing the organisation's objectives by identifying and managing threats and opportunities. Consulting activities include services such as conducting internal control training;

providing advice to management on controls, risk and corporate governance activities; drafting policies or providing assistance; participating in quality teams to determine whether various quality standards are adhered to (for example International Organisation for Standardisation (ISO) International Standards); and many more (McCall 2002:35-37; Anderson 2003:106; Cenker & Nagy 2004:52; Brannen & Cummings 2005:10). The value of a consulting activity is determined by its relevance to its primary stakeholders. For internal auditing, this implies the audit committee, executive management and line management (Campbell *et al.* 2006:45-46; Allegrini, D'Onza, Paape, Melville & Sarens 2006:846-850; Roffia 2007:6). Therefore, internal auditors need to keep close to these stakeholders to be of real value to the organisation.

The use of the word consulting could be misleading. Consulting usually refers to situations when experts or professionals are contracted in to provide a service in a specific field (Oxford Dictionary 2005:247; Wikipedia n.d.(e)), usually from an outside source. However, recognising a constant need for certain expertise has supported the establishment of internal consulting units where organisations set up their own internal consulting group for a specific area or cluster of areas ranging from IT, to training, internal auditing, and even assisting in the development of systems, processes, etc. (Johri & Molnar 1989; Johri, Cooper & Prokopenko 1998; Meislin 2002; Lacey & Tompkins 2007; Vault n.d.). Internal consulting could include the establishment of an internal audit function (White 2007:61-64) as an internal consulting unit; thus providing consulting services as an add-on to the traditional assurance services. The IIA took note of this new way of interpreting consulting and included it in the formal definition of internal auditing.

Although consulting activities have broadened the duties that management entrusts to the internal audit function, there is also a threat linked to this new role, namely the jeopardising of the independence of the internal auditors (refer to section 2.6.1 on p. 113 for a discussion). The IIA has anticipated this problem by suggesting that individuals performing a consulting activity may not perform assurance services on that activity for the next year (IIA 2009(a):18). Whether this is sufficient to ensure independence and objectivity is debatable as certain

consulting activities may have a longer effect on the operations of the organisation.

2.4.1.2 Adding value

Another aspect of the revised definition is the value-adding function of internal auditing. The definition envisions internal auditors who focus on adding value by facilitating improvement through advice and counsel, including both assurance and consulting activities to (normally) all stakeholders within the organisation. In some cases they would even provide assurance to parties outside the organisation, for example, trading partners (IIA 2006(a):13). Research (McCall 2002:36; Deloitte & IIA (UK and Ireland) 2003; Maher & Akers 2003:39; Van Peursem 2004:390; Roffia 2007:3-4; PWC 2008(a)) has indicated that the concept of value-adding for internal auditing is directly linked to the relevance of the activities performed by the internal audit function to management. This is evident from the fact that the performance of consulting engagements by internal auditors is increasing.

2.4.1.3 Corporate governance and risk management

The revised definition expands the scope of internal auditing with regards to assurance, consulting and value-adding to recognise its key role in corporate governance and risk management, in addition to control activities. Although the original purpose of internal auditing was to provide assurance concerning historical activities in the organisation, management's concept of internal auditing broadened over the years, which required internal auditors to broaden their views to include assistance with current and future events. Internal auditors should thus understand their organisation’s business strategy to be able to fulfil this new role. The role of internal auditing in corporate governance and risk management is discussed in Chapter 4.

Figure 2.2 on p. 74 schematically explains the various dimensions of modern internal auditing as noted in the current definition and discussed above.

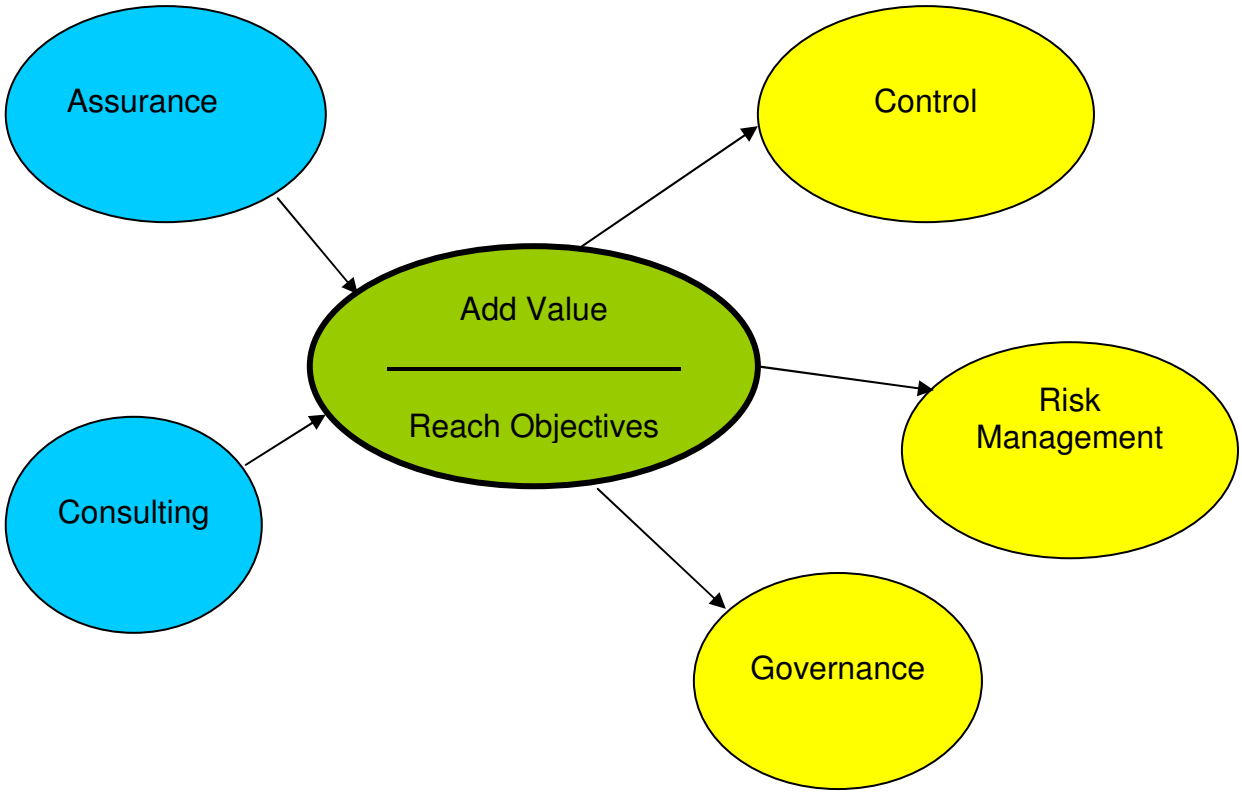


Figure 2.2: Various dimensions of modern internal auditing

2.4.1.4 Necessity of the changes in the definition

The current definition was needed to keep up with the expectations that management has of the internal audit function. As the internal audit function is a service division within the organisation, management's needs must be used to guide the activities of the function. Firstly, providing only assurance to management that policies and procedures implemented by them are adhered to by employees, is very limited. Management also expects internal auditors' input in improving these policies and procedures, and if needed, assistance with the implementation and the monitoring of the improvements. For internal auditors to still be objective and appear as independent when performing assurance services, guidance was needed on how to perform consulting activities without compromising independence and objectivity. Secondly, being a service division, the internal audit function has to add value to the organisation on a strategic as well as operational level. Lastly, although internal control is the core knowledge area of internal auditors, the concepts of corporate governance and risk

management are vital in assisting management to steer the organisation in the right direction. As such, internal auditors need to provide assurance and consulting to management on all three of these areas to be able to add the ultimate value to all stakeholders.

Although the current definition has broadened the role of internal auditing, the profession and individuals must take note that stakeholders' expectations may change as new aspects arise. According to a recent study performed by the IIA Research Foundation (2009(c)) on the effect of the current financial crisis on the profession, many signs could alert the chief audit executive that stakeholders, especially management, are not satisfied with the internal audit function's services. Such signs include less communication from the audit committee and executive management, budgets being cut, pressure to undergo an external quality assessment, to name but a few. Internal auditors' first priority is to keep up with changes affecting their organisations, and to make sure that these are addressed accordingly.

2.4.2 In-house, outsourcing and co-sourcing

Outsourcing is the term used for transferring a process to an outside party and co-sourcing is transferring only a part thereof (IIA 2009(a):2). According to a study performed by the Outsourcing Institute, a global network of researchers and professionals in the field of outsourcing, almost every industry has turned to the benefits of outsourcing (cited in Figg 2000:50). In general, the reasons behind this trend include the reducing and controlling of operating costs as a result of economic pressure, improving organisation focus on core activities, or gaining access to world-class capabilities to increase quality (Figg 2000:50-51; Spencer Pickett 2003:17,596; Ahlawat & Lowe 2004:149-150; Subramaniam *et al.* 2004:90-91; Carcello, Hermanson & Raghunandan 2005:72-74; Van Peursem & Jiang 2008:220; Schneider 2008:16; iKUTU 2009:30-38).

For internal auditing, outsourcing or co-sourcing refers to the appointment of external consultants, for example, external audit firms, to provide the internal audit activities or part thereof for the organisation. This concept has grown so

tremendously that the IIA has issued a position paper to provide guidance to their members when considering outsourcing or co-sourcing (IIA 2009(b)).

Most of the above reasoning could be applicable when deciding whether the internal audit function or part thereof should be outsourced or co-sourced. Although internal auditing is a prominent element of sound corporate governance principles, it may happen that, together with other services such as security, it is sometimes regarded as being a non-core activity in countries where corporate governance is not optimally addressed (Gavin & Matherley 1997:121; Selim & Yiannakas 2000:225; Figg 2000:50; Van Peursem & Jiang 2008:220). Management may argue that by outsourcing the function, more resources could be allocated to core activities (Figg 2000:50; Van Peursem & Jiang 2008:221). However, effective outsourcing is not likely to be less expensive than in-house activities, and thus may have no effect on resources (Selim & Yiannakas (2000:216).

A further rationale supporting outsourcing is that it is sometimes impossible to appoint internal auditors in one organisation with all the necessary skills and knowledge. Many research studies (Subramaniam *et al.* 2004:93; Carey, Subramaniam & Chua Wee Ching 2006:24; Schneider 2008:18; Van Peursem & Jiang 2008:234; iKUTU 2009:30-38) indicate that management may be of the opinion that outsourcing or co-sourcing could provide the means to have access to this knowledge and skills without increasing the internal audit budget. This argument is further supported by the CBOK study (IIA Research Foundation 2007:258), which indicates that when there is a skills shortage within the function (refer to section 2.6.3 on p. 119), 51.4% of respondents use co-sourcing or outsourcing to compensate for the missing skills.

Lastly, outsourcing could mean that a smaller organisation may be able to afford a smaller internal audit component whereas it would be impossible to implement an in-house internal audit function (Schneider 2008:18).

The above arguments may sound as if outsourcing is the ideal solution for the problems in the modern business world. The organisation gets access to

specialists, can focus on its core activities while saving costs and no impairment of the independence of the internal audit function is risked.

There is, however, a down side to outsourcing or co-sourcing an internal audit function. The first concern relevant to this study is the possible lack of independence for the whole audit component (Van Peursem & Jiang 2008:224); especially when the outsourced internal audit activities are performed by the organisation's external auditors. A second concern is the lack of knowledge of the business (especially complex business processes) as well as the lack of relationships and networks compared to a structured in-house function (Schneider 2008:20; Van Peursem & Jiang 2008:220). The iKUTU study (2009:34) adds to the list of advantages of having an in-house function by identifying factors such as internal auditing being a training ground for internal auditors and other employees, as well as better confidentiality. Lastly, the study (iKUTU 2009) concludes that the chief executives as well as audit committee chairs of the top forty SA companies, although both ranked as *very to extremely satisfied*, rank in-house functions as more valuable than outsourced activities with regard to competency, commitment, effectiveness of services, flexibility to accommodate management needs, value adding and fulfilling expectations (iKUTU 2009:72). With regard to the types of activities performed, areas such as corporate governance, risk management, control operational effectiveness, reputation and forensic investigations are also ranked higher for the in-house function (iKUTU 2009:73-74).

With regard to the possible jeopardising of the auditor's independence, the Enron scandal is a relevant example. Arthur Andersen was both the internal and the external auditors and their internal audit fees were more than their external audit fees (refer to section 1.3.4 on p. 17). After the company went bankrupt, SOX (USA – 2002:S201) forbad the practice of external auditors also providing internal audit services. However, during a study performed by Carey *et al*. (2006:21), it was noted that 75% of companies listed on the Australian Stock Exchange outsource internal auditing to their external auditor. In SA, the Companies Act (SA – No 71 of 2008) introduces the concept of an audit committee from a legal perspective for certain companies. In terms of Section 94(7) of the Act, an audit

committee should determine the nature and extent of any non-audit services that the external auditor may provide to the organisation. In addition, Section 93(3) prohibits an external auditor performing services when there is a conflict of interest; this could include the performance of both internal and external audit services. These two sections could have a profound impact on the outsourcing of internal audit services to external audit firms.

With regard to the concern related to the outsourced consultant's lack of knowledge of the business, the following arguments prevail. Firstly, when dividing all internal audit activities into the three key areas, namely financial, compliance and operational, the Carey study (2006:24) found that the traditional services of financial statement auditing and compliance auditing are more commonly chosen for outsourcing. Operational-related activities (that is improving the activities of the organisation) remain predominantly in-house audit services as knowledge of the business is a crucial element in these types of audit engagements. For example, when performing an environmental audit, the improvement of the processes will most probable be done by an in-house function or may be co-sourced. However, the compliance audit may be outsourced completely if so determined by the chief audit executive and management. Secondly, within certain areas knowledge seems to be lacking. In a study performed by PWC (2008(b):12) on the future of the internal audit profession, it was concluded that risk management and IT are specialised fields. IT outsourcing has grown in popularity as an efficient and cost-effective way to meet IT management demands such as systems implementation, maintenance, security and operations (Subramaniam *et al.* 2004:90; Carey *et al.* 2006:24-25).

Many research studies (Subramaniam *et al.* 2004:93; Carcello *et al.* 2005:81-82; Carey *et al.* 2006:26-28; Schneider 2008:21-24; iKUTU 2009:25) have identified that larger organisations are co-sourcing as a convenient and cheaper alternative to increasing the size of the internal audit function to supplement the existing expertise and technological know-how. The above studies also reveal that it often happens that smaller organisations, which are adopting internal auditing for the first time, implement internal auditing through outsourcing and thereafter move to co-sourcing and possibly in-house functions.

With these arguments for and against outsourcing the internal audit function, with regard to this study the question remains whether it could have an effect on the role of internal auditing in the risk management framework as well as risk-based internal audit engagements.

2.4.3 Specialisation fields

The changing profile of the internal audit profession has resulted in a change in knowledge, skills and competencies expectations from the business environment. Apart from the changes within the internal audit environment, a study performed by Ernst & Young (2009(b)) on the mega trends that will influence the world identified the increasing challenge of attracting, managing and developing talent to ensure a global workforce as one of seven critical problems facing business today. According to Harrington (2004:5), Oxner and Oxner (2006:53), and Sumners and Soileau (2008:7-9), an expanded set of skills and competencies is needed by internal auditors to cope with the massive changes and increasing complexity in both private and public sector operations.

Firstly, an expansion in the knowledge and skills of the so-called traditional activities is needed, for example internal auditors must demonstrate expertise in areas such as control evaluations, operational reviews and systems analyses (Ramamoorti 2003:9-13; Oxner & Oxner 2006:56). According to the IIA (2007(a)), a broad range of skills and expertise, and ongoing professional development is needed to ensure the formation and maintenance of an effective internal audit function. This document highlights a few essential elements, namely an in-depth knowledge of the organisation's industry; technical understanding and expertise; skills for implementing and improving processes in both financial and operational areas; strong communication and presentation skills; the profession's standards and best practices. This is substantiated by the CBOK study (IIA Research Foundation 2007:327) that adds ethics and fraud awareness to the list.

The competency framework or CFIA (IIA n.d.(f)), highlights four specific areas of competencies and knowledge that internal auditors should possess, namely:

- tools and techniques;
- knowledge areas, e.g., financial accounting, finance, ethics and fraud;
- internal audit standards, theory and methodology; and
- interpersonal skills.

Apart from the expansion of the generally accepted knowledge and skills of internal auditors, stakeholders now expect internal auditors to assist their organisations in assessing risk management frameworks and processes, developing creative solutions to complex business challenges and exploring new technologies, to name but a few (Pryal 2008:41). To be able to participate and add value to these areas, internal auditors are forced to have at their disposal knowledge and skills in certain specialised fields. Many studies have highlighted, *inter alia*, the following fields as areas in which internal auditors play a crucial role and expert knowledge is needed (Deloitte & IIA (UK and Ireland) 2003:14-19; IIA Research Foundation 2007:344-349; Ernst & Young 2007:2; Pryal 2008:41; PWC 2007:30; PWC 2008(a):31; PWC 2008(b):31-37; Deloitte & IIA (UK and Ireland) 2008:17; Ernst & Young 2008:11-13):

- risk management;
- governance;
- fraud prevention;
- IT management assessment;
- data mining and analysis; and
- specific industry skills including risk identification and assessment.

The two specialisation fields for internal auditors that are identified as crucial in most of these studies are risk (refer to Chapter 4 for a detailed discussion) and IT (refer to section 2.6.6 on p. 126). Although the studies highlight different areas within these two fields as being more important than others, overall IT and risk are identified by the respondents more than any other field as being specialised fields. This is substantiated by the result of a comprehensive study performed by PWC (2008(b)) on the future of internal auditing. The results of this study not only identify the two fields as being specialisation fields, but also emphasise the

shortage of internal auditors with the necessary competencies and skills in these fields (refer to section 2.6.3 on p. 119 for a discussion). Lastly, the third King Report on Governance (IOD 2009:15-16) highlights risk-based internal auditing and IT governance as two emerging trends and as such added since the issuing of the second report.

The IIA must take notice of these specialisation fields and provide their members with appropriate guidance. Although the *Standards* and practice advisories do address most of these areas (IIA 2009(a)), more detailed guidance in the form of practice guides is needed. Currently, most of the topics included in the practice guides (refer to section 2.4.4.1 on p. 81) that are relevant to the above list of specialised fields cover IT (IIA 2009(a):xii-xiii). There are none covering the risk-related field. The IIA should take note of this and more detailed guidance should be developed.

2.4.4 Professional guidance

Much new guidance has been published to assist internal auditors with all the changes that have affected their activities. Most of these are mentioned in section 1.2.4 on p. 9. This section elaborates on this guidance with specific reference to the study.

2.4.4.1 International professional practices framework

After the current definition was proclaimed in 1999, the need for a new structural professional guidance became evident. The IIA Inc. has developed guidance in the form of the IPPF that consists of six elements (IIA 2009(a):iv) that are now briefly discussed with specific reference to their importance to this study:

- **Definition of internal auditing (mandatory)**

The definition (IIA 2009(a):xvi) of internal auditing is the umbrella under which the rest of the elements fall and states the purpose, nature and scope of the profession (refer to section 2.4.1 on p.70 for a detailed discussion).

- **Code of ethics (mandatory)**

A code of ethics (IIA 2009(a):xvi) has been established to promote an ethical culture throughout the internal audit profession. It states the principles for conduct and expectations regarding the behaviour of individuals and internal audit functions in the conduct of internal audit activities. The code applies to all internal auditors performing internal audit services, regardless of the industry and the changing business environment.

- **International standards for the professional practice of internal auditing (mandatory)**

The *Standards* (IIA 2009(a):xvi) provides the minimum requirements to be maintained by internal auditors for acceptable practice within the profession. It consists of various criteria by which the activities of internal auditing are evaluated and measured. The *Standards* document has been restructured to align it with the current definition of internal auditing and it now has a much broader perspective, prescribing a proactive role for internal auditors not only in control activities, but also in risk management and corporate governance processes. As the *Standards* are mandatory, it will be referred to where applicable in the rest of the study.

- **Practice advisories (strongly recommended)**

These guidelines (IIA 2009(a):xvii) include specific topics that currently require attention and may have a limited life or may be included in the formal *Standards*, depending on importance, usage and acceptance. The guidelines assist internal auditors in applying the rest of the IPPF, and include approaches, methodologies, considerations and interpretations. Although not mandatory, the practice advisories are detailed discussions on various topics, and will be referred to where applicable in the rest of this study.

- **Position papers (strongly recommended)**

These documents (IIA 2009(a):xvii) are not only for the use of internal auditors, but for all stakeholders to understand the roles and responsibilities of internal auditing in matters such as control, governance and risk management processes. Currently (July 2010), the IIA has only two position papers, of which one is on the role of internal auditing in risk management. This document, although not compulsory, is incorporated in this study as a risk mature organisation will most probably strive to implement all its guidance (refer to section 4.3.1.1.1 on p. 235).

- **Practice guides (strongly recommended)**

The practice guides (IIA 2009(a):xvii) are detailed guidance on a specific topic. They consist of detailed procedures and processes, which include techniques, programmes and approaches that are obtained through educational publications, research studies and other relevant material. Hopefully, this study's outcome may contribute to the profession by being included in the practice guides as a tool when performing risk-based internal audit engagements.

2.4.4.2 Other Institute of Internal Auditors guidance

Other guidance that could have an influence on this study includes:

- CBOK – refer to section 1.2.4.2 on p. 9.
- CFIA – refer to section 1.2.4.3 on p. 10.
- Organisational governance: guidance for internal auditors – refer to sections 1.2.4.4 on p. 10 and 4.2.1.2 on p. 229.
- IIA position paper on the role of internal auditing in enterprise-wide risk management issues – refer to sections 1.2.4.5 on p. 11 and 4.3.1.1.1 on p. 235.
- IIA (UK and Ireland) position paper on risk-based internal auditing – refer to sections 1.2.4.6 on p. 11 and 4.3.3.1.2 on p. 248.

- Internal audit capability maturity model for the public sector – refer to section 4.3.1.1.1 on p. 235.

2.4.5 Conclusion

The internal audit profession has undergone many changes in the last few decades, starting with a new definition that reflects the elements of a modern internal audit profession. Because of this expanded role of internal auditing, management has taken note of the value that an effective internal audit function can add, being it in-house, outsourced or co-sourced. Management is expecting more of its internal auditors and specialised fields such as IT and risk are beginning to form an essential part of the skills and knowledge requirements of competent internal auditors. The IIA has developed new guidance to assist their members with this new demand. The question is whether the guidance is adequate to address the need, specifically for risk management and related areas.

2.5 EXTERNAL FACTORS AFFECTING THE INTERNAL AUDIT PROFESSSION

Many factors outside the internal audit profession have had, and are still having an effect on how internal auditing is perceived. It is important for the profession to take note of these as this will ultimately affect the way the internal audit functions are utilised. This in turn will affect the way internal auditors perform their duties and will ultimately affect internal audit methodology, including the performance of internal audit engagements. The most important aspects addressed in this section include globalisation, corporate governance, and the various stakeholders of internal auditing and how they recognise the value of internal auditing.

2.5.1 Globalisation

The physical location of an organisation, country boarders, citizenship and other logistics are no longer obstacles for the business environment. With the concept of globalisation, activities such as communication, travelling, the sharing of

information and data, and the distribution of inventory are easier and faster. International growth, the expansion of the economic markets, uplifting of developing countries and the never-ending search for lower costs, are some of the reasons why globalisation is here to stay.

Two examples where globalisation could be beneficial to the day-to-day operations of an organisation are now explained. First, organisations outsource low-level activities to third-world countries at a fraction of the first-world cost (Ramamoorti & Weidenmier 2003:334). An example is where documents are electronically sent to a worker in another country. After the worker has performed his/her procedures on the documents, he/she sends them back to the organisation. Secondly, globalisation could also assist with the distribution of knowledge and skills. For example, when an international organisation needs a specific skill for a project to be performed in country X, the individual(s) that possesses that skill is re-located to country X for the duration of the project. This will result in skills being available when and where needed, but also at a possibly lower cost, as each country where the organisation resides does not have to appoint individuals with all the needed skills.

The IIA has grasped this new way of thinking and has positioned itself in a global internal audit organisation serving members through its chapters and affiliates worldwide (refer to section 1.2.1 on p. 5 for a discussion), whose objectives all include the words ‘global’ or ‘worldwide’ (IIA n.d.(a)). The CBOK study (IIA Research Foundation 2007:29) supports the reasoning of the IIA in being a global profession as 39.2% of the respondents’ employers operated in an international environment.

But how does globalisation affect the day-to-day activities of the internal audit function and the individual internal auditor? At first glance it seems that globalisation could only be a positive movement for the profession. A few advantages include one body governing the profession, internal auditors being in an ideal position to add the most value to their international organisations structure as the *Standards* and methodology are applicable worldwide, and the

CIA designation being recognised globally. There are, however, some disadvantages and concerns to take note of.

Studies performed by Ernst & Young (2007:8 and 2008:14-16) and a study performed by PWC (2008(a):13-20) identified the following challenges for globalisation:

- difference in language and culture;
- political risks;
- complexity of operations;
- lack of local knowledge, for example, laws, regulations and accounting standards;
- internal auditors' reluctance to travel frequently;
- lack of quality and standards;
- increase in internal audit costs; and
- increase in the work load of the internal audit function.

Although 41% of respondents in the Ernst & Young (2007:8) study indicated that their organisations have international activities and a centralised internal audit function situated in the global headquarters, only 34% of these respondents were satisfied with their coverage of the international activities. According to Hofstede (cited in Ellingson 2009:50-53), globalisation also has an influence on how people perceive risk. As a result of various studies performed, he developed an Uncertainty Avoidance Index (UAI), which measures a specific society's level of uncertainty or risk appetite. According to this model, people from different cultural backgrounds have different levels of tolerance for uncertainty with, for example, the USA having a higher risk tolerance than the world average and Japan having a lower risk tolerance. This will have a direct influence on how risk are treated and managed by an organisation within a specific culture; thus influencing the activities of the internal audit function.

A further concern is 'job-hopping' (Christopher, Sarens & Leung 2009:209). As a result of the increase in the activities of the internal audit function, internal

auditors with specific competencies are scarce. Such internal auditors with the right knowledge and skills are headhunted on a frequent basis. With globalisation, one governing body, one qualification and one set of guidelines, it is easy for an individual to re-locate to another country. Countries (or organisations) that put in a great effort to educate and train these internal auditors could lose their knowledge and skills to other countries (or organisations) as a result of the skills shortages.

Globalisation is here to stay and it has an enormous effect on the internal audit profession that should be geared to serve the organisation in a global environment. Internal audit functions should take note of the potential challenges and position the function in such a manner that the advantages it provides are fully utilised. Internal auditors, when performing internal audit engagements, should be aware of the possible risks related to international operations.

2.5.2 Corporate governance and internal auditing

In section 1.3 on p. 12 the concept of corporate governance is briefly introduced. In this section, the development of corporate governance with regard to internal auditing is investigated. The discussion includes the development of corporate governance codes and other guidance and legislation, and their influence on the internal audit profession. Corporate governance with reference to internal auditing in an SA context is highlighted, as well as the effect of corporate scandals on the profession (refer to section 3.2 on p. 138 for a discussion of corporate governance and its relationship with risk management and section 4.2 on p. 228 for the role and responsibility of the internal auditor).

According to leading organisations across the globe such as the NYSE (Harrington 2004:1) and the USA's National Association of Corporate Directors (Staciokas & Rupsys 2005:170), and the Institute of Directors (IOD) in SA (IOD 2002:23-41), internal auditing, together with executive management, audit committees and external auditing, forms the cornerstone of effective corporate governance. This statement is supported by many research studies involving boards of directors, senior management and internal audit functions (Deloitte &

IIA (UK and Ireland) 2003; Gramling, Maletta, Schneider & Church 2004; Crowe Chizek 2005; Crowe Chizek 2006; Krell 2006; PWC 2008(a); PWC 2008(b); Marx 2008; iKUTU 2009:34).

Some of the countries that recognise internal auditing as being part of sound corporate governance are listed in table 2.3 on p. 89 (IIA n.d.(h); Green & Gregory 2005:50-54; Jackson 2005(b):345-350). These examples are an indication that internal auditing is being recognised for the important role it could play in corporate governance. It is therefore important for the internal auditors to ensure that they do not fail to impress the business environment with what they can contribute to this topic. Many documents and research studies have been conducted on the role of internal auditing in corporate governance. These are further debated in Chapter 4.

It is, however, important to note that the implementation of certain requirements will have an effect on whether the internal audit function will be successful in contributing to the corporate governance process or not. The internal audit function's existence cannot be a mere 'tick off' of the corporate governance list of requirements (refer to section 2.6.2 on p. 117). Aspects (Paape, Scheffe & Snoep 2003:253-257; Gramling *et al.* 2004:197-199; iKUTU 2009:88-90) such as the quality of the internal audit function, the structure of the function, the implementation of the function within the organisational structure, the relationship between the function and other parties such as the external auditors, the audit committee and executive management, the position or status of the function within the organisation, resources allocated to the function, to name but a few, will all either contribute or hinder the internal audit function in its participation in the corporate governance system of the organisation.

Table 2.3: Inclusion of internal auditing in global corporate governance guidance

Country	Body	Internal Audit Function
Australia	Australian Stock Exchange	Audit committee which drives internal audit
	Australian Prudential Regulatory Authority	All financial institutions
Canada	Canadian Federal Government	Recognises IIA *Standards*
China	Government	Laws and regulations on internal auditing
India	Stock Exchange Board	All listed companies
Italy	Italian Stock Exchange	Management code for listed companies
Kenya	Nairobi Stock Exchange	Listed companies
Malaysia	Code of Corporate Governance	Public listed companies
Mexico	Government	Public sector organisations
Netherlands	Code of Corporate Governance	Listed companies
	Government	Public sector organisations
Norway	Financial Services Authority	Large banks and insurance organisations
SA	Government	Public sector organisations
	Johannesburg Stock Exchange	Listed companies
	Code of Corporate Governance	All organisations
Spain	Comision Nacional del Mercado de Valores	Listed companies
Sweden	Government	Government agencies
Taiwan	Government	Public companies must have at least one internal auditor
United States	New York Stock Exchange	Listed companies

(Source: refer to discussion)

To assist the organisation in implementing and maintaining sound corporate governance systems and processes, many guidelines in the form of corporate governance codes, legislation and general documentation are being issued, these are discussed in the next section.

2.5.2.1 Corporate governance codes

The corporate governance codes issued worldwide are in a constant state of development as change takes place in the business environment and new problems emerge, for example, corporate scandals (Spencer Pickett 2004(a):24-25; IFAC 2004:14-16). As a result of this, and the fact that internal auditing is recognised by various role players as an asset to corporate governance, it is included in most of the newly issued governance reports (ECGI n.d.; Drew *et al.* 2006:128).

According to the European Corporate Governance Institute (ECGI n.d.), on 9 April 2008, there were two hundred and twenty eight corporate governance codes issued by sixty four countries and five *ad hoc* bodies to provide organisations within specific countries or for specific areas, for example, the commonwealth, with guidance. Although many new corporate governance codes are issued on an ongoing basis, some of these new codes add to the evolution of the concept of corporate governance. In table 2.4 on p. 91, some of the developments in the evolution process are summarised by referring to the most prominent global codes with specific reference to internal auditing (Commonwealth Association for Corporate Governance (CACG) 1999; Corporate Governance Committee 2003; Spencer Pickett 2003:47-59; De Castro 2005; Lewis 2007; Marx 2008:97-205).

Although not all these codes or documents enforce an internal audit function on organisations, they encourage management to make use of internal auditing as a tool to assist with certain responsibilities. The last document in table 2.4, namely the third King Report (IOD 2009) issued by the IOD in SA, has the most comprehensive section on the establishment of an internal audit function (13% of the total report) and is discussed in section 2.5.2.3 on p. 96.

Corporate governance codes are viewed by many as the main type of guidance available on corporate governance principles as most countries do have some form of corporate governance code (ECGI n.d.). There are, however, other forms of guidance as discussed in the next section.

Table 2.4: Evolution of corporate governance codes and related documents with regard to internal auditing

Year	Code	Country	Topic added
1987	Treadway	USA	Internal control with reference to internal auditing
1992	Treadway (COSO)	USA	Internal control with specific reference to the role of internal auditing
1992	Cadbury	UK	Internal audit function complementary to external auditors
1994	King I	SA	Internal audit function recommended
1994	Dey	Canada	Audit committee direct communication with internal auditing
1996	Bosch	Australia	Internal audit unrestricted access to audit committee
1998	Hampel	UK	Internal audit function supported
1999	Turnbull	UK	Companies that do not have an internal audit function should review the need for one
1999	Malaysian	Malaysia	Head of internal auditing must attend all audit committee meetings
2002	King II	SA	Internal auditing compulsory or board must disclose reasons for non-compliance
2003	Smith (Combined Code)	UK	Audit committee should review effectiveness of internal audit function
2003	Dutch Code (Tabaksblat)	Netherlands	Internal audit function compulsory and accountable to management board
2004	Treadway (COSO)	USA	Enterprise risk management with specific reference to the role of internal auditing
2006	Combined Code	UK	Audit committee oversee internal audit If no internal audit function: • audit committee review needed annually • report in annual report
2007	Revised Code	Australia	Consider having internal audit. Function linked to proper risk management process.
2009	King III	SA	Internal auditing compulsory or board must disclose reasons for non-compliance and explain how assurance has been maintained

(Source: refer to discussion)

2.5.2.2 Other corporate governance–related guidelines and legislation

There is much relevant guidance, but only the most prominent and those that have an influence on internal auditing are discussed in this section.

- **Principles of corporate governance**

The Organisation for Economic Cooperation and Development (OECD 2004) is an international organisation of thirty countries that endorses the principles of representative democracy and free-market economy. The OECD Principles of Corporate Governance were endorsed by OECD ministers in 1999 and have since been applied internationally by policy makers, investors, corporations and other stakeholders. The corporate governance agenda provides specific guidance for legislative and regulatory initiatives in both OECD and non-OECD countries.

Throughout this document internal auditing is described as the right-hand of the board and senior management. Although the responsibility for activities remains with management, it is suggested that internal auditing should be used to assist them with this task. It also claims that in order for the level of oversight by senior management to be appropriate and sufficient, internal auditing should report directly to the board (OECD 2004:62), enhancing the independence and effectiveness of the internal audit function (refer to sections 2.6.1 on p. 113 and 2.7 on p. 130).

- **Commonwealth Association for Corporate Governance**

The Commonwealth Association for Corporate Governance (CACG 1999) was established in 1998 to promote sound corporate governance principles in the commonwealth, of which SA is a member country. The CACG had developed fifteen broad principles with regard to corporate governance. The principles are based on the input of various corporate governance codes and other guidelines, and most of these do include reference to internal auditing.

- **Committee of Sponsoring Organisations Report – Internal Control**

The Treadway Commission's Committee of Sponsoring Organisation report for the USA issued in 1987 (COSO 1992), identified control as the most important mechanism that management can use to ensure that its plans and procedures are adhered to. The COSO was asked to conduct a review of internal control as a result of the findings of the Treadway Commission's report (COSO 1992). The Committee called for organisations to work together to integrate the various internal control concepts developed and used by different organisations and to develop a common point of reference for internal control. The purpose of the COSO study was to provide a common understanding of internal control among all parties and to assist management in exercising better control over an entity. The result was a report, *Internal Control – Integrated Framework*, issued in 1992. The study developed a comprehensive definition of control, namely (COSO 1992:3):

> Internal control is a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - effectiveness and efficiency of operations;
> - reliability of financial reporting; and
> - compliance with applicable laws and regulations.

The first category focuses on the reaching of an organisation's business objectives, including the identification and management of risks. The second category looks at the data gathered and used in the decision-making process and financial statements. The third category examines compliance of laws and regulations to which the organisation is subject.

According to the report, internal auditing is one of the leading parties in assuring that these guidelines are functioning properly (COSO 1992:88-89), with its main responsibility being reviewing the various activities and providing assurance to management that the internal control framework is implemented as dictated by them. This document is further discussed in section 4.5.4 on p. 268 as it formed a

part of the evolution of how internal audit engagements were, and in some cases still are, performed.

- **Committee of Sponsoring Organisations Report – Enterprise Risk Management**

The second COSO Report on enterprise risk management was published in September 2004 (COSO 2004) and focuses on enterprise risk management and controls as a tool to help manage risks threatening an organisation. This document is a comprehensive guideline on how to manage risk in an organisation and is used as one of the guidelines in establishing a risk management process (refer to section 3.5 on p. 191 for a detail discussion).

The role of internal auditing (COSO 2004:88) is summarised as evaluating the effectiveness of the process and recommending improvements. This document is also used in the development of a risk-based internal audit engagement as discussed in section 4.5.4 on p. 268.

- **Risk management standards**

Various organisations have issued standards on risk management, including the Institute of Risk Management (IRM) (2002), the Australian Standards Board and the New Zealand Standards Board (AS/NZS 2004), and ISO (2007). These all emphasize that risk management is an integral part of good corporate governance practice, explain the process of risk management, and provide guidance on how to establish an effective risk management framework.

The above documents all emphasise the fact that the risk management framework should be monitored and reviewed for effectiveness. The IRM (2002:13) stipulates that internal auditing is in the best position to fulfil this task by, *inter alia*, focusing their activities on significant risks identified and providing assurance on the risk management process (these documents are discussed in section 3.5 on p. 191 – development of a risk management process).

- **Sarbanes Oxley Act**

The Public Accounting Reform and Investor Protection Act of 2002, referred to as SOX (2002), was promulgated on 30 July 2002 by the USA government. The Act was a response to the corporate scandals that influenced the American economy during the years preceding the Act (refer to sections 1.3.4 on p. 17 and 2.5.2.4 on p. 103).

Section 404, being the most applicable to internal auditing, requires management to develop and monitor procedures and controls for making their assertion about the adequacy of internal controls over financial reporting, as well as the required attestation by an external auditor of management's assertion. Section 302 requires management's quarterly certification of not only financial reporting controls, but also disclosure controls and procedures.

It is management's responsibility to ensure that the organisation complies with the requirements of the Act, but support for management in the discharge of these responsibilities is a legitimate role for internal auditors (IIA 2004:3). In addition to the increased focus on the internal audit function's support role with regard to risk management, control and governance processes, the requirements of SOX have created benefits such as enhanced management awareness of risks and controls, a stronger control environment, and a potential reduction in external audit fees (IIA 2004:9). Refer to section 3.2.3.3 on p. 149 for a discussion on the debate of rules- or principle-driven corporate governance guidelines.

According to a study performed by Elson and Lynn (2008), chief audit executives confirm that SOX has had an impact on USA's internal audit functions. This includes the initial implementation of Section 404 requirements, and the continuous testing of the compliance thereof. The study (Elson & Lynn 2008:63) also reveals that as a result of the Act, internal auditing is more involved in corporate governance aspects in general, with specific areas including ethics, business conduct, legal and regulatory compliance.

- **New York Stock Exchange corporate governance rules**

The NYSE (2003), like most other similar bodies worldwide, is constantly revising their listing requirements. In their requirements, as amended in 2009, all listed companies must have an internal audit function (NYSE 2003:13) and the audit committee must oversee the responsibilities of the function. In addition, the requirements stipulate that audit committees must meet privately with the internal auditors on a regular basis, enhancing the independence of the internal audit function (NYSE 2003:12).

2.5.2.3 Corporate governance in South Africa

SA has not lost track of the global developments in corporate governance. Both the private sector and to a lesser extent the public sector contributed to the implementation and improvement of not only corporate governance in general, but also the establishment of internal audit functions within organisations.

The investigations undertaken by the IOD's King Committee were prompted by the initiatives stipulated in table 2.4 on p. 91, and the first King Report on Corporate Governance (IOD 1994) was issued on 29 November 1994, with a second report following on 1 March 2002 (IOD 2002), and a third issued on 1 September 2009 (IOD 2009).

The three King reports (IOD 1994, 2002, 2009) contain sets of recommendations that represent the minimum practices that should be adopted by a board of directors as part of their corporate governance code of practice. According to the first and second reports, the recommendations are directed at all companies listed on the JSE Limited, the SA stock exchange, at corporations falling under the SA Finances Services sector, and organisations that perform public functions (inclusive of those regulated by the PFMA and the MFMA). All other organisations are encouraged to adopt the principles as far as possible (KPMG 2003(a)). The third report (IOD 2009:17-18) evolved even further. It applies to all organisations regardless of the manner and form of incorporation or establishment. The committee argues that all organisations adhering to the code will practice sound

corporate governance and therefore encourages all organisations to incorporate the principles.

All three King reports address the aspect of establishing an internal audit function. In table 2.5 on p. 99 the evolution of the three King reports with regard to internal auditing is highlighted (IOD 1994:21-22, 2002:86-90, 2009:92-98).

King I (IOD 1994:21-22) only briefly includes the importance of establishing an internal audit function. However, King II (IOD 2002:86-90) contains comprehensive coverage on the importance of a well-establishment effective and efficient internal audit function. In this document, emphasis is placed on the fact that risk, control and corporate governance are the responsibility of the board of directors and senior management, but simultaneously recognising the role of the internal auditor by incorporating the *Standards* of the IIA regarding these aspects (IOD 2002:76,88).

In the third King Report (IOD 2009), comprehensive coverage is provided on the establishment of an internal audit function. Various additional aspects are included, namely (refer to table 2.5 on p. 99; Deloitte 2009; Ernst & Young 2009(c); PWC 2009; Van Wyk 2009):

- the positioning of the internal audit function within the organisation to understand the strategic directions and goals of the organisation, including the reporting line to the audit committee (refer to section 2.6.1 on p. 113);
- the outsourcing of the function (refer to section 2.4.2 on p. 75) due to a shortage of skills (refer to section 2.6.3 on p. 119) and the organisation focusing on core activities (refer to section 2.4.2 on p. 75);
- quality review of the function that enhances the effectiveness of the function's activities;
- broadening the role of the audit committee as overseer of the function enhancing independence (refer to section 2.6.1 on p. 119);
- enhancing the function's role in providing a written assessment of the system of internal control, including the financial controls;

- enhancing the function' role in risk aspects by establishing:
  - interaction with the board's risk committee (refer to section 3.3.6.1 on p. 177);
  - the function's year-plan based on risk and addressing the full spectrum of organisational risks, identifying areas of high priority, providing assurance on effectiveness of the risk management process, and assessing the risk maturity of the risk management framework (refer to section 4.3 on p. 232); and
  - the assessment of the organisation's strategic risks and opportunities (refer to section 4.3.1 on p. 234);
- addressing the competency, skills and knowledge requirements of the internal audit staff (refer to sections 2.4.3 on p. 79 and 2.6.3 on p. 119);
- broadening the scope of activities to include ethics- and fraud-related aspects; and
- internal auditing being part of the overall assurance model of the organisation.

The third King Report's increased recognition of internal auditing as a necessity for sound corporate governance was a welcome statement by a highly respectable institution. The various King reports are cited by many national and international organisations and individuals as one of the best codes on corporate governance (Gray, Coetzee, Chambers – CEO of IIA Inc. cited in Baker 2010:31-32). It is further refreshing to see that the new additions mostly focus on enhancing the standing of the internal audit function within the organisation. The one specialisation area for internal auditors that is greatly uplifted in the report is risk-based internal auditing. This is further debated in Chapter 4 of this study.

Table 2.5: Evolution of internal auditing with reference to South African corporate governance codes

Topic	King I	King II	King III
Requirement	• Recommended	• Part of corporate governance • If not implemented, report reasons in annual report	• Requirement • If not implemented, report reasons in annual report and how assurance is maintained
Responsibility	• N/A	• Board and executive management	• Board and/or its committees
Status	• Must command respect	• Must command respect • Independence	• Respect and cooperation of board • Strategically positioned to achieve objectives • Independence *via* audit committee (CAE confirm annually) • CAE standing invitation to attend sub-committee meetings
Structure	• N/A	• N/A	• When outsourced, senior executive must be custodian
Reporting	• Recommend report to audit committee chair	• Administratively to CEO • Functionally to audit committee chair	• Functionally to audit committee chair • Provide assurance to the board • Report at level allowing independence from management/meets management and audit committee requirements
Board relationship	• Recommend access to board chair	• Access to board chair	• Respect and cooperation of board and management • Standing invitation to attend sub-committee meetings
Quality review	• N/A	• N/A	• Develop and maintain plan • Audit committee ensure independent review in line with *Standards*
Audit committee	• N/A	• Attend all meetings	• Approve internal audit charter • Working relationship • CAE reports at meetings • CAE meets with audit committee chair prior to and after meeting

Topic	King I	King II	King III
			• Internal audit provide assessment of governance, risk and control • Internal audit function's plan endorsed
CAE	• N/A	• Appoint by audit committee	• Appoint, assess and dismiss by audit committee
Staff	• N/A	• N/A	• Serve complex area of business and provide greater value • Address risk and assurance needs • Technical and business skills including tools and techniques • Appropriate competencies with regard to control and risk spectrum
Resources	• N/A	• N/A	• Audit committee responsible for sufficient resources / budget
IIA	• Adopt *Standards*	• Adopt *Standards*	• Adopt *Standards* and Code of Ethics
Industry	• N/A	• N/A	• Appropriate industry competencies and knowledge
Role and function	• N/A	• Assist executive and senior management	• Address emerging business, organisational, operational and assurance needs via flexible and dynamic processes • Provide assurance on combined assurance framework • Assess effectiveness of control, performance and risk management • Written assessment of control and risk management effectiveness
Scope	• Review: ○ reliability and integrity of information ○ systems ○ safeguarding assets ○ reach of objectives • Appraise economic, efficient, effective conduct	• Risk management • Control • Governance	• Risk-based audit approach • Risk management and internal control framework • Business processes and controls (financial, operational, compliance and sustainability aspects) • Governance, including ethics and tone at the top • Source of information with regard to fraud, corruption, unethical behaviour, irregularities

The requirements of the King reports, especially King III (2009) should be applied by both the private and the public sectors. In the next two sections, additional corporate governance requirements for each of the two sectors are discussed.

2.5.2.3.1 Private sector

Although the King reports do not have legal status in SA, the JSE Limited has adopted the principles as mandatory for all listed companies as from 1 September 2003 (Baue 2003). Currently this implies compliance with the requirements as set out in the second King Report (IOD 2002). The third King Report will be effective from 1 March 2010. Future research could include the investigation on the effect of these more extended requirements on the functioning of internal auditing.

- **Companies Act**

As explained in section 1.3.2.1 on p. 15, the new Companies Act, No 71 of 2008 (SA – 2008) has been promulgated on 9 April 2009. Although internal auditing is not mandatory, it is mentioned under Section 94(7) that the audit committee is…

> to deal appropriately with any concerns or complaints, whether from within or outside the company, or on its own initiative, relating to… the … internal audit of the company.

- **Bank Act**

The Bank Act is industry-specific guidance, however, as the financial sector is currently in the lime-light as a result of the credit crunch and the accompanying worldwide financial crisis (refer to section 2.6.5 on p. 123), the legislation applicable to this sector is briefly discussed. According to the Bank Act, No 94 of 1990 as amended in 2003 (SA – Banks Amendment Act, No 19 of 2003) of SA, the audit committee is the overseer of the internal audit function. Although the implementation of an internal audit function is not mandatory according to the Act,

the Basle Report (Basle Committee 2004:30) enforces an independent and effective internal audit function.

2.5.2.3.2 Public sector

After the issuing of the first King Report (IOD 1994), the government of SA decided to implement corporate governance principles for the public sector. Although striving to adhere to the King Report's requirements, government has to operate in a strict legislative environment. In 1999, the PFMA was promulgated and became mandatory for all national, provincial and public-held government organisations (SA – No 1 of 1999), followed by the Protocol on Corporate Governance in the Public Sector (SA – Department of Public Enterprises 2002) for public-held organisations, and the MFMA for municipal organisations (SA – No 56 of 2003). These documents are discussed with specific reference to the implementation of an internal audit function.

- **Public Finance and Management Act and Treasury Regulations**

According to the PFMA (SA – 1999:S76(e)) and the Treasury Regulations that were issued in terms of the PFMA (SA – National Treasury 2005:3.2), all government organisations must have an internal audit function. The audit committee must review the effectiveness and activities performed by the function, enhancing the independence of the function. Other aspects included in the Act and the Treasury Regulations include the establishment of an audit charter, adopting the IIA definition and *Standards* as requirements for performing internal audit activities, and detailed responsibilities and tasks of the function.

A point related to this study is that a risk assessment must be performed by management on a regular basis and that a risk management strategy, based on the risk assessment, must guide the internal audit function's priorities (SA – PFMA 1999:S38(1); SA – National Treasury 2005:3.2). This is further debated in Chapter 4 of this study.

- **The Protocol on Corporate Governance in the Public Sector**

This document (SA – Department of Public Enterprises 2002:30-31) is specifically for public-held entities and elaborates on the stipulations of the PFMA. Although the Treasury Regulations include the possibility of departments sharing internal audit functions (SA – National Treasury 2005:3.2) this document adds that the "majority of internal audit staff should be full-time employees of the organisation", eliminating the possibility of outsourcing but still allowing the possibility of co-sourcing (refer to section 2.4.2 on p. 75).

- **Municipal Finance Management Act**

The MFMA (SA – 2003:S62) enforces the establishment of an effective, efficient and transparent internal audit function for all local authorities. Section 165 of the Act addresses the duties and responsibilities of the function. According to Section 165(2)(a), the internal audit function's year-plan must be based on risk, again making this Act relevant to this study (this is discussed in section 4.3.2 on p. 242).

2.5.2.4 Corporate scandals affecting internal auditing

Although corporate collapses and business failures are not new phenomena (refer to section 1.3.4 on p. 17), it is important to evaluate the role internal auditing played when these scandals occurred. In most of the biggest corporate scandals (Markham 2006:212), the external auditors, either issuing clean audit reports proceeding the scandals, or being involved in a more negative way, for example, not performing crucial activities, are prominently mentioned in scandals such as Enron, Tyco, Global Crossings, Adelphia and WorldCom. Another factor playing a key role in many of the scandals is the lack of internal controls (Bookal 2002:46; Spencer Pickett 2003:37-45; IFAC 2004:13-19; Markham 2006:661). However, in most instances internal auditing is not mentioned. In the next sections, the involvement of the internal auditors and the role they have played,

either in discovering the problem or fraud, or not discovering wrongdoings that should have been obvious, are briefly discussed.

2.5.2.4.1 Some major global corporate scandals

Internal auditing's involvement with most of these scandals is limited. Internal auditing does however have some concerns in the aftermath of some of the major global corporate scandals. The first concern is when internal auditors do perform their tasks properly but management choose to ignore their advice, for example, the case of Bearings Bank. The bank, being the UK's oldest merchant bank, collapsed due to a lack of proper internal controls (Spencer Pickett 2003:39). An internal audit report was issued to top management warning them that there was a significant risk with regards to the proper segregation of duties of Nick Leeson, the manager in both the back and the front office of the treasury department of the bank. The recommendation by internal auditing was ignored and the result was the collapse of the bank. This raised the concern as to whether recommendations made by the internal audit function are taken serious by management. According to a study performed in Australia on the role of internal auditing in corporate governance (Leung *et al*. 2003), only 20% of internal auditors felt that their recommendations were considered or implemented by management. Contradictory to this, in an SA study (iKUTU 2009:93) performed amongst audit committee chairs, 32% indicated that the recommendations received from the internal audit function are always implemented and 64.3% are frequently implemented. This could be as a result of the strong guidance on internal auditing in the King reports.

A second concern is the question of independence of the internal and external audit services as a result of outsourcing activities (refer to section 2.4.2 on p. 75). An example is the Enron scandal. As discussed in section 1.3.4 on p. 17, Enron was one of the biggest corporate scandals with the internal audit function outsourced to the organisation's external auditors, namely Arthur Andersen. When examining the history of the Enron debacle (Markham 2006:95-142), it is understandable why Arthur Andersen chose to ignore the red lights. The internal audit fees exceeded the external audit fees by $2 million and the auditors were

afraid of losing one of their biggest clients. Although the practice of using a specific audit firm as both outsourced internal auditors and external auditors was discouraged (in the USA, made law) as a result of this scandal, it is still a common practice in certain countries, for example, Australia (Carey *et al.* 2006:21).

Followed on the footsteps of Enron, came WorldCom, a further scandal affecting the USA economy. In contrast to the above concerns, the internal audit function's chief audit executive, Cynthia Cooper, was the whistleblower that brought the fraudulent activities of the telecommunication giant to a stop (Cooper 2008). After several attempts of various parties such as the chief financial officer and even the audit committee chair to keep her from probing into the organisation's affairs, she continued her struggle to bring the wrongdoings to light. A study performed by, *inter alia*, the IIA (Australia) amongst chief audit executives (Leung *et al*. 2003:33) concluded that only 54% of internal auditors feel free to report malpractices without jeopardising their positions. This is confirmed in a study by Hughes (2004:3) where over a third of internal auditors expressed the opinion that they could lose their jobs or have in the past been pressured to quit their position due to being the bearer of bad news or the pursuer of information that was felt to be to the detriment of top executives.

2.5.2.4.2 Some South African corporate scandals

SA has had its fair share of corporate scandals, both in the private and the public sectors (Vaughn & Verstegen-Ryan 2006; Fraser-Moleketi 2008; Khoabane 2009). Although no specific example could be linked to the internal audit function, much was written on the subject of scandals as a result of poor corporate governance policies and the role that internal auditing should play. Still, many contradicting facts are available on the aspect of sound corporate governance *versus* the occurrence of scandals. In 2003, the Institute of International Finance rated SA amongst the best performers in corporate governance in emerging markets (cited in Vaughn & Verstegen-Ryan 2006:511). Unfortunately, as cited in Newsome (2004:28), in 2002 the Corruption Perception Index rated SA at number thirty six out of a hundred and two countries.

Former president of the IIA (SA) and a board member of the IIA Inc., Rob Newsome (2004:26-31), asks whether a scandal the size of Enron could occur in SA. He argues that although SA has some of the best corporate guidelines and legislation in the world, many organisations are slow in implementing these strategies. This is echoed by Khoabane (2009) regarding the recent discovery of one of the latest scandals rocking the government, namely the ruling party or African National Congress (ANC) spokesman Carl Niehaus confessing to accumulating massive debt and fraudulent activities. The Minister for Public Service and Administration, Ms Fraser-Moleketi (2008), addressing senior members of the private and public sectors, urged stakeholders (including internal auditing) to stand up and address the problem:

> Corruption in both the private and the public sector poses important socio-economic, governance and values and ethics challenges in contemporary South Africa…. Internal audit acts as an important preventative measure against fraud. South Africa has realised the value and importance of internal audit….

Although internal auditing is not, as in the case of Enron, linked to a corporate scandal in a negative way, the definite link between internal auditors and the prevention or detection of major scandals in SA could not be made. Globally, the profession is recognised by many stakeholders as one of the key factors in addressing this concern. SA, with the various corporate codes and legislation driving the internal audit profession, is in an ideal position to assist management with the prevention and/or detection of corporate scandals. Still, in SA, as in the rest of the world, corporate scandals do occur in both the private and the public sectors with the arms deal being one of the biggest scandals in the history of the SA government (Feinstein 2007). This raises the question as to where the internal auditors were in preventing and/or detecting the irregularities that caused the scandals.

2.5.3 Recognition of internal auditing by role players

Many stakeholders in the business environment recognise that internal auditing is a key player in corporate governance. This is proved by the fact that internal

auditing is included in prominent corporate governance guidelines and legislation (refer to section 2.5.2 on p. 87). The stakeholders' recognition will have an effect on the utilisation of the internal audit function, which will in turn influence the investment that management and the board are prepared to make in the function, influencing the quality of the function. Cumulatively, this must have an effect on the internal audit profession and the type of individuals that want to become internal auditors; completing the circle as this again influences how stakeholders perceive internal auditing. This section discusses the results of a few studies on how various role players perceive internal auditing, including parties from within as well as outside the organisation.

2.5.3.1 Parties within the organisation

Internal auditors are employed by management, report to management and have as their main objective to assist management in reaching the organisation's objectives. How internal auditing is regarded by management as well as other co-employees is an indication of how well they succeed in this task. The parties that have the closest link with internal auditing are the board of directors and its committees, as well as top management including line management (Guner 2008:25-27).

2.5.3.1.1 Board of directors and its committees

The main function of internal auditing with regard to the board of directors is to provide them with assurance on organisational activities *via* its board committees, especially the audit committee. It is thus important that, for the internal audit function to be effective in performing this task, the function should be structured in such a manner that it could function independently from the management team (refer to section 2.6.1 on p. 113). The independence and status of the internal audit function will ultimately affect the relationship with the board and the audit committee as internal auditors will have greater confidence in reporting wrongdoings to them. Zain and Subramaniam's (2007:899) study indicates that 91% of the chief audit executives interviewed declared that the audit committee

protected the internal audit function in instances when they were frank and open about problems.

According to a study where chairpersons of audit committees (iKUTU 2009:88) were interviewed as to their satisfaction with the contributions of the internal audit function, levels varied from 'very' to 'extremely' satisfied. A notable result of this study is that respondents (representing both the audit committee chair as well as senior management) indicated a difference in the contribution of in-house functions and the contribution of outsourced functions, with a significant higher level of satisfaction with the in-house function from the audit committee (refer to section 2.4.2 on p. 75). This could be an indication that the board, which is represented by the audit committee, regards information related to the organisation's business environment and functioning (which is one of the main advantages of an in-house internal audit function) as more relevant than senior management does. This is probably a result of management being part of the daily activities of the organisation and having a more comprehensive understanding of the organisation's functioning, whereas the board is composed of executive as well as non-executive members, with the latter having a limited knowledge of the organisation's activities.

2.5.3.1.2 Senior management

Although internal auditing should be directly responsible and accountable to the board and its audit committee (IOD 2009:95-96), day-to-day activities are performed in conjunction with the management team. Senior management expects internal auditing to fulfil certain tasks, ranging from assurance to consulting activities (most of these are included in the formal definition of internal auditing – refer to section 2.4.1 on p. 70). In a study performed in Belgium (Sarens & De Beelde 2006(b):219-241) of five prominent organisations, management indicated that they were satisfied that the function was meeting these expectations. A study in SA (iKUTU 2009:96-97) concludes that chief executive officers are extremely satisfied with the internal audit function with regards to aspects such as competency, commitment, effectiveness of service, flexibility to accommodate management's needs, value adding and meeting

management's expectations. This is supported by a study (Carcello *et al*. 2005) on the investment by senior management in USA public organisations in internal auditing. The study concludes that one of the major factors contributing to the positive view of senior management regarding the internal audit function is the (Carcello *et al.* 2005:82) contribution of internal auditing in managing the risks of the organisation.

2.5.3.2 Parties from outside the organisation

The most important stakeholder external to the organisation's corporate governance operations is the shareholders or, in the case of the public sector, the general public, followed by the external auditors, government and other regulators (Guner 2008:27-29). How internal auditing is viewed by these stakeholders is briefly discussed here. Proof of regulators enhancing the role of internal auditors by means of legislation is discussed in sections 2.5.2.2 on p. 92 and 2.5.2.3 on p. 96 and will not be included in this discussion.

2.5.3.2.1 Shareholders

Internal auditors' main objective is to assist management. External auditors, however, are appointed by shareholders as agents to provide them with an opinion on the true and fair representation of the financial statements (refer to section 2.3 on p. 63). The relationship between external auditors and shareholders is an established one. However, the value that shareholders link to an effective internal audit function is debatable as reflected in the research performed on this topic. According to De Zoort, Hermanson and Houston (2003:186) and Guner (2008:27) the lack of this relationship is soon to be changed as shareholders want to exercise closer oversight and control of management and corporate decision-making. Internal auditing is in the perfect position to provide a bridge between these two parties (refer to figure 2.1 on p. 69). After numerous corporate scandals affecting the economy worldwide, external parties losing their confidence in the markets (Markham 2006:39-400) and the possible positive contribution of the internal audit function in restoring

confidence (Ernst & Young 2007:2; West 2009:10), the profession could also play a possible role in restoring the confidence of shareholders.

According to a study by Paape *et al.* (2003:251), shareholders expect internal auditing to provide detailed information on financial and non-financial indicators on management activities and future organisational risks. 68% of bank lenders interviewed in a study performed by James (2004:17) indicated that an effective internal audit function is of great to maximum importance to the reliability of an organisation's financial statements. Holt and De Zoort (2009:61,71-72) tested whether a descriptive internal audit report affects investors' confidence and decisions. The study concludes that adding an internal audit report to the existing reports issued with the financial statements increases the investors' perception of the effectiveness of the oversight and their confidence in the financial reporting reliability. The internal audit report has the same value as the audit committee report and managements' reports, with the external auditors' reports, as can be expected, leading the way.

The possible contribution that internal auditing could make in restoring shareholders' confidence could broaden the current role of internal auditors as the right hand of management (internal party) to include a wider function on providing assurance externally. In contrast to the external auditors that primarily provide assurance on financial information, the internal audit report should include the measure of operational effectiveness, including the management of risks.

2.5.3.2.2 External auditors

For the private sector, SAICA, the SA governing body of the external audit profession, stipulates that the external auditor may only make use of the work performed by the internal auditor after the following has occurred (SAICA 2009/10:ISA610-2 to 6). The external auditor must:

- determine if the work performed by the internal auditors is adequate for the purpose of the specific audit, with specific reference to:

- the internal audit function's objectivity;
- the internal auditors' technical competencies;
- the work performed with due professional care;
- effective communication between the internal and external auditors;

- determine the effect of the internal auditors' work performed on the work to be performed by the external auditors, with specific reference to:
  - nature and scope of the work;
  - assessed risks of material misstatements;
  - the degree of subjectivity when evaluating the audit evidence;
- evaluate the work performed on a specific internal audit engagement that the external auditor wants to rely on, including:
  - the technical competencies and skills of the internal auditors;
  - proper supervision and reviews occurred and documentation exists;
  - sufficient and appropriate audit evidence was obtained;
  - conclusions are in line with the audit work performed; and
  - any unusual matters or exceptional circumstances were revealed and resolved.

The above establishes that the external audit profession does provide a platform for its members to use the work of the internal auditors. Studies indicate that there is a greater tendency of external auditors to use the work performed by the internal auditors than in the past (Apostolou, Harper & Strawser 1990:309; Gramling 1999:124; Gramling *et al.* 2004:233; Haron *et al.* 2004:1156). The latter study (2004:1158) indicates that this is as a result of the improvement of the quality of the internal auditor's training programme and the satisfactory follow-up procedures in prior audit engagements. Gramling *et al.* (2004:210) state that the quality of internal audit functions is the key factor determining any reliance the external auditor may place on the internal audit work. Morrill and Morrill (2003:495,501) declare that the external auditor's use of the internal audit function increases substantially where audit-specific knowledge is required, thus the internal audit function's well planned staffing and structure could enhance this relationship.

In SA, the Public Audit Act (SA – No 25 of 2004), when stipulating the activities of the Auditor General (refer to section 1.4.2 on p. 21), does not mention the coordination between the Auditor General and the auditee's internal audit function. However, the International Standards on Auditing issued by the SAICA does make provision for a public sector perspective (SAICA 2009/10:Background-3) applicable to registered auditors performing audits of financial statements in the public sector. A further document issued by the International Public Sector Standards Board (IFAC 1994:9-12) on guidelines when using the work of other auditors, identifies similar considerations for the public sector when using the work of the internal audit function.

Although the SA Auditor General is, with good reason, reluctant to rely on the work performed by the public sectors' internal audit functions (refer to section 1.4.2 on p. 21), and the documents on standards mentioned above do include requirements for registered auditors performing financial statements audits in the public sector on using the work of the internal audit function, the question remains why this is not addressed in the legal requirements of the Auditor General. Although government external auditors use the SAICA guidelines, other types of activities that are more relevant to the public sector, such as performance auditing, are not included in this guidance.

2.5.4 Conclusion

From the above discussion it is evident that the internal audit profession operates within a complex network. It is one of a few professions that are globally managed, providing national and international organisations' management teams with an assurance tool that, if structured and managed properly, can be very useful in enhancing corporate governance. Although corporate governance is not a new invention or discovery, it has, over the last few decades, evolved to a widely recognised concept. With internal auditing being part of corporate governance, playing a crucial role in preventing and discovering corporate scandals, and being recognised by various stakeholders as a key role-player, the profession has to live up to expectations. Threats to the profession need to be

identified and addressed before they can harm the improved recognition internal auditing currently receives.

2.6 THREATS TO THE INTERNAL AUDIT PROFESSION

With the changes and new dimensions in internal auditing, threats to the profession also evolved. Some of the current threats that could have the most impact on the profession are briefly discussed. These include the independence of the internal audit function and objectivity of the internal auditors, corporate governance requirements, competencies, knowledge and skills required of internal auditors, the scope of the role of the internal auditors, the current global financial crisis, and lastly, technology.

2.6.1 Independence

Internal auditing will always operate within the contradicting facts of, on the one hand being a part of the organisation, and on the other hand trying to remain independent and objective (KPMG 2003(b):2-3; Crowe Chizek 2005:3; Crowe Chizek 2006:3). The independence of the internal audit function and objectivity of the internal auditor are enhanced by various factors – the most important being the reporting lines. According to the IIA (IIA 2006(a):41-44) and reports issued by other major role players (IOD 2002:186; KPMG 2005:26-32; ECIIA 2005:28; Crowe Chizek 2006:2; Marx 2008:291), the chief audit executive should report operationally or functionally to the audit committee and administratively to the chief executive officer, enhancing not only the independence and status of the function, but also the fact that internal auditing is part of the corporate governance structure. Most applicable legislation, codes and other standards (SA – PFMA 1999:S77; IOD 2002:78-82; IIA 2006(a):100-101; SA – Companies Act 2008:S94; IOD 2009:56) highlight the independence of the audit committee, making this line of reporting the ideal route to follow for internal auditing.

The independence and status of the internal audit function are crucial elements in the effectiveness of the activities performed by the function. According to the third

King Report on Governance (IOD 2009:97 – own emphasis), internal auditing must be strategically positioned to accomplish their objectives:

> Companies should have an **effective** internal audit function that is **independent and objective.** Internal audit should **report functionally to the audit committee** to ensure this and should have the **respect and cooperation** of both the board and the management.

Although studies performed globally in the public sector (refer to section 1.5.1 on p. 24) confirm that this reporting structure is mostly applicable, the statistics on the private sector are contradictory. Various studies indicate a lower rate for private sector internal auditing reporting to the audit committee and senior management (Zain & Subramaniam 2007:899; Christopher *et al.* 2009:209-211). In a study performed in Australia amongst chief audit executives (Christopher *et al.* 2009:211), only 38.24% of the respondents report functionally to the audit committee and 32.35% report administratively to the chief executive officer. A concerning result is that 26.47% reports to the chief financial officer, possibly undermining the independence of the internal auditor as discussed in section 1.5.1 on p. 24. This is supported by Green and Gregory (2005:59) who find that USA organisations, although exhibiting a clear trend that chief audit executives are changing their reporting lines to report to the audit committee, still report in many instances directly to the chief financial officer. Other studies indicate a higher rate for private sector internal auditing reporting to the audit committee and senior management. According to studies performed by PWC (2007 and 2008(a)) on the latest trends in global internal auditing, 81% (2007:42) and 89% (2008(a):7) of the respondents indicated that the internal audit function do report functionally to the audit committee and 88% reported that the function reports administratively to the chief executive officer. These statistics, although a lower adherence rate is indicated, are also confirmed by the CBOK study (IIA Research Foundation 2007:185), which concludes that 54% of the respondents report to the chief executive officer and 51% to the audit committee. Lastly, in the PWC study on the future of internal auditing (2008(b):41) respondents foresee an increase in chief audit executives reporting to chief executive officers.

In SA, the study performed by Van der Nest (2006:196) concludes that all chief audit executive respondents in the public sector report to the audit committee, possibly referring to functional reporting structures. For the private sector, a study performed by Marx (2008:433) on audit committees in larger private sector companies concludes that all audit committees review the findings of the internal audit function, possibly referring to functional reporting lines. The study also concludes that 94% of the respondents indicated that the internal auditors have unrestricted access to the chair of the audit committee, with a possible 6% contradicting the previous assumption. A study performed by iKUTU (2009:23,27) amongst the audit committee chairs and other executives of the top forty companies listed on the JSE Limited reveals data supporting the independence of the internal audit function with 83.3% of functional reporting occurring to the audit committee as per corporate governance guidelines. There are, however, many concerns. Firstly, the fact that chief executives and audit committee chairs do not agree on the reporting lines of the internal audit function is concerning (iKUTU 2009:19,22). It would have been expected at least that these two parties know to whom the chief audit executive reports to. Secondly, the fact that many chief audit executives report administratively to the chief financial officer (iKUTU 2009:19,22) is contradictory to their independence as many of the internal audit functions activities occur within the financial sphere of the organisation (refer to section 1.5.1 on p. 24).

Most probably due to legislative requirements, the above statistics regarding reporting lines put the public sector in a better position than the private sector. However, whether this fact is beneficial to the internal audit function, remains to be seen. It could be that the public sector, being driven by legislation, is only adhering to compulsory requirements (refer to section 2.6.2 on p. 117 for a discussion) without adhering to the principle of the King Report (IOD 2009:97) as quoted above. The private sector, although not adhering strictly to the guidelines, may be more focused on enhancing the independence of the internal audit function by implementing reporting lines best suited for its individual needs.

A further concerning factor that could possibly influence the independence of the internal audit function is the additional consulting role of internal auditors. As

discussed in section 2.4.1.1 on p. 71, the addition of consulting activities to the internal audit function scope has widened the spectrum of duties to be performed by internal auditors. The board of directors relies on the assurance services performed by, *inter alia*, the internal audit function. According to Chambers (2008:47-63) boards are in urgent need of proper assurance as they are too often caught by surprise when their policies are not being implemented by management or by events that occur that were not on their high-priority list, such as the current financial crisis. The internal audit function is in the ideal position to assist the board by monitoring organisational activities and reporting its findings to the board *via* the independent audit committee (Bou-Raad 2000:184-185; McCall 2002:35; Van Peursem 2004:378; Cenker & Nagy 2004:50; Fraser & Henry 2007:403). When consulting activities increase, assurance services most probably will have to decrease (refer to figure 2.2 on p. 74 for the input elements) as a result of limited resources. Additionally, the function's independence and objectivity will most probably be affected when performing assurance activities on the areas where consulting activities were performed previously; even with the *Standards* suggesting a one-year interruption before such services can be performed (IIA 2009(a):18). This means internal auditors will, for example, provide assurance on controls that they have implemented. The internal audit function should take note of these possible problems related to how they spent their time and manage it accordingly by planning ahead. The audit committee as extension of the board should also take note of these aspects as the internal audit function's year plan must be approved by senior management and the board (IIA 2009(a):26).

Research performed by the IIA (New Zealand) amongst their members revealed that although consulting activities are performed on a regular basis, most participants recognised the conflict between these duties and the independence of the internal audit function (Van Peursem 2004:380-384). Various other researches confirm management are aware and expect that the duties to be performed by internal auditing are changing. This includes the movement from assurance to consulting activities; providing advice on or taking responsibility for the risk management process; and identifying crucial risks threatening the achievement of the organisation's objectives (McCall 2002:35-37; Deloitte & IIA

(UK and Ireland) 2003; Paape *et al.* 2003:255; Cenker & Nagy 2004:52; Brannen & Cummings 2005:10; Allegrini *et al.* 2006:846-850; PWC 2007:9; IIA Research Foundation 2007:53).

From the above, it is clear that internal auditing has an important role to fulfil to meet the needs of its stakeholders. Management expects the internal audit function to provide them with advice on demand, leaning more to a consulting role, whereas the board's expectations of the internal audit function are more of an assurance provider. It seems, from research performed (Van Peursem 2004:384; Brannen & Cummings 2005:10; Allegrini *et al.* 2006:850), that management's needs are getting preference to those of the board. The IIA should take note of this conflict, and although applicable guidelines do exist in the form of practice advisories on consulting activities (IIA 2009(a):55-60), more comprehensive guidelines may be required, for example, guidelines on how to define the limits of consulting activities, advice on proper communication between the relevant parties, possibly revising the audit charter, and guidelines on how to prioritise between assurance and consulting activities. This includes the role of the internal audit function with regard to risk management and is discussed in Chapter 4 of this study.

2.6.2 Corporate governance requirements

Admirable steps have been taken over the last few decades to improve corporate governance. Many documents on sound governance principles exist (refer to section 2.5.2 on p. 87). The USA follows a strict rule-based approach with SOX, as does the public sector in SA as a further example. A 'apply or explain' regime is currently followed by some countries, such as SA (IOD 2009:6-7) and a 'comply or explain' in other countries, for example in certain European countries (Baker 2004(b):16). An example where the latter approach has failed is with the Parmalat scandal. Parmalat, the Enron of Europe, is an Italian company with a complex business and financial structure. In 2004 it was discovered that the financial statements of one of the subsidiaries were misstated, resulting in a great loss for the shareholders (Sverige 2004). In 2001, the organisation declared that

it did not have an internal audit function and explained that (cited in Baker 2004(b):16):

> …the group's existing structure is already sufficiently well organised to manage so-called internal audit procedures….

The question is not whether organisations adhere to the applicable guidelines, be they strictly rules-driven (such as legislation) or principles-driven (such as codes). Studies (Mardjono 2005:282; Markham 2006:596) and other literature (Spencer Pickett 2003:45; Williams 2008:472) indicate that most of the organisations linked to corporate scandals have indicated in various reports that they practiced sound governance principles (refer to section 3.2.3.1 on p. 146). It is rather a question of the effectiveness with which these guidelines were implemented (also refer to section 3.2.3.3 on p. 149 for a discussion on rules-based *versus* principles-based guidance). Was it a mere 'tick off' of a checklist for adherence, or was it implemented to really improve governance? Many believe (Waring 2006:36; Alexakis, Balios, Papagelis & Xanthakis 2006:682; Aluchna 2009:195) that despite the huge effort to provide proper guidance to those involved with the management of an organisation, the truth is that in many instances not much has changed in the day-today activities of certain organisations. This is evident from the following factors:

- continuous number of scandals rocking the business environment, both in the private sector and the public sector (Newsome 2004:28; Mardjono 2005:272; Waring 2006:36-37; Khoabane 2009; Southern African Information Portal on Corruption n.d.);
- the negative correlation between the organisations' corporate governance ratings and their corporate performance (Heracleous 2001:165; Donker & Zahir 2008:92); and
- the weak influence of sound corporate governance on sustainability aspects (Aras & Crowther 2008:441-444).

It seems that even within the organisation's internal environment, the elimination of misconduct is a near impossible task. According to a study performed by

KPMG (2008/9:1) on integrity, three out of four (75%) employees participating in the survey had observed wrongdoings in their organisations within the last year, with the public sector leading with an 80% rate. Moreover, 60% (KPMG 2008/9:2) of the respondents observing wrongdoings in the banking environment reported that their observations would, if the wrongdoings were made public, cause a significant loss of public trust. This most probably refers to potential further corporate scandals.

The above implies that corporate governance cannot merely be implemented to adhere to a checklist; it has to come with the right attitude. For internal auditing, this means the difference between an organisation implementing an internal audit function for the sake of adherence to corporate governance guidelines, and the implementation of an effective internal audit function (refer to section 2.7 on p. 130) that is truly independent (refer to section 2.6.1 on p. 113). Until bodies such as the IIA, in conjunction with regulators and legislators, enforce certain criteria on organisations linked to determine the true effectiveness of the internal audit function, the possibility will always exist that an organisation will have an internal audit function that is ineffective, inefficient and not worthy of the name of a competent internal audit function. Whether such internal audit functions are capable of assisting management in reaching objectives by, *inter alia*, providing assurance on the risk management process and confirming that all risks are addressed, is another debate.

2.6.3 Scarcity of competent and skilled internal auditors

In sections 1.2.2 on p. 6 and 1.2.3 on p. 8 the growth of the profession and the scarcity of competent and skilled internal auditors are briefly mentioned as two contradicting factors. On the one hand there is an enormous growth as evident from the number of new IIA members (refer to table 1.1 on p.7), but on the other hand, studies indicate that there is still a shortage of competent and skilled internal auditors (refer to the percentage of members that are CIAs to substantiate this fact), especially in certain fields. In SA, the Sector Education and Training Authority (SETA) for the Finance, Accounting, Management Consulting

and Other Financial Services sector (Fasset 2007/2008:13-14) supports this finding with internal auditing being recognised as a scare skill for the sector.

Studies performed worldwide identify two main problem areas (Goodwin 2004:644; Ernst & Young 2007:6-7; Singer 2008:7). Firstly, organisations struggle to attract the right mix of talent to be able to meet the needs of all the stakeholders and to add value to the organisation. Secondly, they do not succeed in retaining internal auditors in the internal audit function, therefore losing the chance for them to make a significant contribution. The fact that many organisations use internal auditing as a stepping stone to prepare individuals for managerial positions (Oxner & Oxner 2006:56; Christopher *et al*. 2009:209), places a further burden on the remaining staff.

The scarcity of competent and skilled internal auditors is highlighted by many global studies performed that address aspects such as:

- the technical and soft skills and competencies that are required of tomorrow's internal auditor (McCaul 2006(b):19; IIA Research Foundation 2007:282,290,308,325; PWC 2007:30-31; Ernst & Young 2007:8; Roffia 2007:14; Deloitte & IIA (UK and Ireland) 2008:6-7; PWC 2008(a):28-30; PWC 2008(b):39; Ernst & Young 2008:17);
- internationalisation of the profession and the resource needs that accompany this (Ernst & Young 2007:9; PWC 2008(b):13-20; Ernst & Young 2008:14-15);
- the current salary war and related vacancies in key positions (Robert Half International 2007:7; Roffia 2007:13; PWC 2008(a):30; Harrington 2008:47);
- recruiting and retaining of staff, including staff turnover (Ernst & Young 2007:6-9; PWC 2007:30; Singer 2008:7);
- training and development required (Spencer Pickett 2000:266-268; Siegel & O'Shaughnessy 2008:27; Singer 2008:8);
- the importance of succession planning, especially the chief audit executive position (McCaul 2006(b):18-21);

- the use of staff rotation or the outsourcing of certain activities to provide in the needs of the internal audit function (PWC 2007:32-33; IIA Research Foundation 2007:256,258); and
- future demand as predicted by chief executives and audit committee chairs (iKUTU 2009:100-102).

Although it is a fact that the profession is growing at a tremendous rate, there is a need for more skilled and competent internal auditors. That management is using internal auditing to prepare and train future managers of the organisation is confirmation that the profession is doing something right, but is also a warning light.

It is a commonly known fact in the business environment that growing too fast could be a risk. Is the profession prepared for growth, do internal audit functions have the necessary resources, is quality sustained, do the IIA have the right guidance in place, etc? These are questions that chief audit executives and management within the organisation should ask themselves. On a macro level, these questions should be answered by the IIA.

The fact that skilled and competent internal auditors are scarce indicates two problem areas that need to be addressed. Firstly, more internal auditors must be equipped with the right skills and competencies. The CBOK study (IIA Research Foundation 2007) and CFIA (IIA n.d.(f)) have contributed greatly to identifying the shortages in technical skills (refer to section 2.4.3 on p. 79 for a discussion on specialisation fields) as well as general skills and competencies required. Secondly, management needs to retain the right people by making it worth their while to stay in the internal audit function. A study performed by Harrington (2008) for the IIA on the compensations of internal auditors in the USA and Canada indicates that although the economy is weaker in these countries, internal auditors are still in an excellent position regarding job opportunities and salaries.

The profession is currently viewed positively and it is important to sustain this. The IIA needs to address the skills and competency shortage by providing more guidance, training and uplifting education. A controversial question is whether the entry levels for IIA membership and for the CIA examination should be uplifted from a mere bachelors degree to a higher level. The problem is that although internal auditing is a global profession with the CIA recognised worldwide, each country still has its own education system. For example, in SA, until 2003 (Ttappous 2009(b)), an individual needed to hold an honours degree (four years study and two degrees) to sit for the CIA examination. Members misused the system and travelled to neighbouring countries that had lower entry requirements (for example Botswana only requires a bachelor's degree, thus they were able to sit with only a three-year degree). This forced the IIA (SA) to adjust to a lower entry level. Currently in SA a bachelor's degree is adequate, although the individual must then complete an extra year of practical experience in the internal audit field.

2.6.4 The scope of internal audit activities

The current definition (refer to section 2.4.1 on p. 70) of internal auditing with the inclusion of consulting activities as well as risk and governance processes, has raised a new threat for the internal audit profession. Where does the internal audit function 'draw the line' with regard to activities performed, fulfilling management's needs and making sure there are no new surprises awaiting the organisation? This is especially pertinent considering that one of the biggest complaints of chief audit executives is the limited resources (Deloitte & IIA (UK and Ireland) 2008:4; PWC 2008(b):39; Ernst & Young 2008:11) and the lack of skills available (refer to section 2.6.3 on p.119). In general the business world is becoming more complex, and with aspects such as globalisation (refer to section 2.5.1 on p. 84) and the current global financial crisis (refer to section 2.6.5 on p. 123) and its impact on the internal audit function's resources, the scope of activities performed by the internal auditors may well become an obstacle instead of the current view of progress of the profession.

A further concern regarding the scope of internal audit activities is the use of the internal audit function to assist the external audit process due to cost savings (Mathker 2008). Concerns raised include the fact that the internal audit function's plan is too wide and does not allow internal auditors to focus on their core activities and responsibilities. This is also linked to the use of especially external audit firms as outsourced internal audit providers, where the methodology followed by these parties is criticised as leaning to the external audit methodology.

Internal auditors need to take note of these concerns. To provide a quality service to all stakeholders, they need to make sure that only activities that can be performed with due proficiency (IIA 2009(a):20) should be accepted. This could influence the number of consulting activities accepted (refer to section 2.4.1.1 on p. 71). Furthermore, the scope of activities should be clearly documented in the internal audit charter – the language used should be specific enough to avoid any misinterpretation as a result of vague terminology. Lastly, internal audit activities should be performed more productively, for example, using a structured risk-based internal audit approach.

2.6.5 Global financial crisis

The current global financial crisis is in many ways a shock to the business world; the biggest crisis being that it was not foreseen by economists and other relevant stakeholders, and thus organisations and government could not prepare themselves for what was to come. In May 2007 the OECD made the following statement (cited in Keen 2008):

> … the current economic situation is in many ways better that what we have experienced in years. Our central forecast remains indeed quite benign.

Three months later this statement was contradicted by the USA stock market that went into decline, house prices that fell and organisations that went into serious financial crisis. This was followed by the rest of the world's financial markets and other organisations that ran into financial crisis. The current financial crisis should

not be underestimated. In fact, many dominant world markets, for example, the USA, and the UK, are currently in more dire straits than those of the Great Depression in 1929 (Keen 2008).

Already the public is asking where the auditors were – referring to both internal and external auditors (Mathker 2008; Olah 2009:11; Lubbe 2009). How was it possible that the auditors, with the extent of the current crisis, could not foresee that something drastic was wrong and why did they not warn all stakeholders of the possible risks – especially internal auditing that has to, according to the *Standards*, incorporate risk-related aspects into their daily activities. The types of risks that initiated the global financial crisis are typically only discovered by a sound risk management framework, something that management is responsible for, but internal auditors need to ensure is functioning efficiently and effectively. Ernst & Young's annual business risk report (2009(a):4-5), a survey amongst industry commentators and sector experts, places the global financial crisis and the deepening financial recession as number one and three, respectively, on the list of top ten risks faced by organisations.

How does this affect the internal audit profession? Firstly, like many other organisations, the IIA Inc., the global body of the profession, is in a financial crisis. Richard Chambers, the president of the IIA, informed members globally (IIA 2009(d)) about the body's current position, referring to the stagnating membership growth, decrease in members attending conferences and training courses, and the layoff of staff. This could have an implication on the services provided by the IIA Inc. to their members. Secondly, as the internal audit function is not a core activity of an organisation, management may decide to cut the function's budget – affecting the activities and scope of services. This would mean that internal audit activities would have to be performed more efficiently, thus saving resources. If this is a possibility within a specific organisation, the audit committee's role in aligning the organisation's internal audit needs with the internal audit function's annual plan should increase. For example, the audit committee should ensure that crucial assurance services do not take second place after management consulting services. Thirdly, internal auditors should ask themselves what they could do to assist management during this crisis.

According to two studies performed by the IIA Research Foundation, internal auditors anticipated (2009(a)) and have seen an impact (2009(c)) of the global financial crisis on the internal audit function within organisations. In the first study (IIA Research Foundation 2009(a):1), internal auditors anticipated eight areas where the global financial crisis will most probably affect their activities, namely:

- an increase in fraud detection and prevention;
- a slowdown of new positions, and staff cuts;
- an increase in financial-related audits;
- the extension of audit cycle times due to staff cuts;
- an increase in attention to risk management processes;
- an increase in the review of fundraising activities;
- an increase in the examination of third-party contracts; and
- an increase in management cost-saving initiates.

In the second study (IIA Research Foundation 2009(c)) the research findings indicate the following:

- The economic recession has already impacted certain internal audit functions with about 50% of organisations having budget cuts in their internal audit function.
- Internal auditors are focusing more on emerging risks that result from the changing economic conditions.
- The majority of respondents (56%) disagreed with the statement that better risk management could have prevented the current crisis, yet 40% acknowledged the fact that internal auditing could have done more to assist their organisations in identifying and mitigating key risks.
- The expectations of stakeholders are changing and have an influence on the internal audit function.

Although the above indicates that the current financial crisis is destructive for the profession in general, the upside is that this could probably open management's eyes to the contribution that internal auditing could make to the management of

risk. According to the 2008 global internal audit survey performed by Ernst & Young (2008:5-8), management are calling on internal auditors to increase their focus on strategic and operational risks, supplementing their current activities on compliance and financial risks. This is confirmed by the IIA Research Foundation study (2009(a):8-9) and it is echoed by government, especially in the USA, for example, the USA Federal Reserve Board of Governors and the USA Department of Homeland Security (cited in Beasly 2009:61), calling for the integration of strategy and risk management, and a more effective risk management process.

This is a move in the right direction, but it is concerning that a crisis of this scale was needed for management to take note. The business environment and corporate governance regulators need to understand that the complexity of the modern world means management need a new mechanism to assist in the running of an organisation. A comprehensive risk management framework may well be the answer, with internal auditing playing a crucial role.

2.6.6 Technology

In sections 2.4.3 on p. 79 and 2.6.3 on p. 119, the specialised knowledge required from modern internal auditors and the threats to the profession as a result of this, are respectively discussed. This section focuses on the influence of technology, specifically IT, as one of the possible biggest threats or foes to the profession. According to a study performed by Ernst & Young (2009(b)) on the global mega-trends to be expected in the near future, the innovation of technology is one of seven topics identified. The internal audit profession cannot ignore this relevant and dynamic area. In a study performed by Ramamoorti and Weidenmier (2004:301-377) for the IIA Research Foundation on the pervasive impact of IT on internal auditing, it is concluded that IT plays a dual role. Firstly it is a driver, referring to the fact that internal audit engagements will have to focus on the importance of IT-related aspects in an organisation, both strategically as well as operationally (refer to number 1 to 6 in table 2.6 on p. 128). Secondly, it is an enabler, assisting the internal auditor with performing activities (refer to number 5 to 9 in table 2.6 on p. 128).

Many studies (Addison 2001; Pang 2001; Ramamoorti & Weidenmier 2004:315-327; Jayalakshmy, Seetharaman & Wei Kong 2005:269; Abu-Musa 2006:438-460; Roffia 2007:9-12; Ernst & Young 2008:20-26; Filipek 2007:29-33; Sumners & Soileau 2008:7-8; Clemmons 2009:16; iKUTU 2009; Mantey 2009:41-43; IT Governance Institute n.d.) incorporate this field in their investigation of modern internal auditing. Table 2.6 on p. 128 summarises the most prominent areas where internal auditing is affected, as well as the possible threat or advantage linked to each area (please note that this is not a comprehensive list).

From the information gathered in these studies, it is evident that the biggest single threat to the internal audit profession with regard to IT is the lack of knowledge, skills and competencies. In the study performed by Ernst & Young (2008:13), 51% of participants indicated that IT auditing skills are the most difficult to recruit. Only 22% (Ernst & Young 2008:17) of respondents agreed that their staff is competent when using technology. A study performed by Deloitte and the IIA (UK and Ireland 2008:13-14) indicates that chief audit executives admitted to a limited use of Computer Assisted Audit Tools and Techniques (CAATTs) and continuous audit techniques (28%), as well as declaring that IT-related risks are not understood (understanding limited to infrastructure (34%), applications (38%) and assurance (41%)). PWC's (2008(b):45-50) study on the future of the profession in 2012 highlights IT as one of five emerging trends for the profession. Respondents supported the fact that technology will play an even bigger role in years to come with 95% expecting IT to impact the organisation in general as well as the internal auditors' ability to strengthen the internal audit process, 79% believe that IT related risks will pose an increased danger for the organisation, and 100% predict the increase in use of IT. Strategies to address this new trend all include the need for IT resources, and eight out of ten include skills and competencies of internal auditors.

Although the IIA has taken note of this new trend and need as reflected in the number of position papers and practice guides (IIA 2009(a):xii), much more will have to be done to narrow the gap between what is currently the practice (Deloitte & IIA (UK and Ireland) and Ernst & Young studies) and what is needed by 2012 (PWC study).

Table 2.6: Technology affecting the internal audit profession

	Area	Explanation	Threat	Advantage
1	IT governance	• Strategic alignment of business and IT objectives. Internal audit must provide assurance on system development and acquisition, implementation, maintenance, assets and data safeguarding	• Lack sufficient knowledge of business and/or IT systems • Brings new risks to organisation • Not assisting optimum IT capabilities	• Can prevent purchase and implementation of system not promoting strategic objectives • Provide clear directions for IT investment, e.g., resources • Assist with alignment of IT operations with operational objectives • Assist with management of IT risks • Assurance on IT services provided
2	IT legislation	• Laws and regulations to manage and control IT-related aspects. Internal audit must provide assurance	• Not aware of all possible legislation	• Adherence will control certain other risks related to IT, e.g., privacy of information
3	Operational risks and controls	• The daily activities of the organisation using IT systems and processes. Internal audit must include in their audit assurance engagements	• Focus on traditional risks not including IT-related risks	• Can test the system faster • Efficient control will be consistent – no/lower manual mistakes/fraud
4	Data security	• Data integrity, privacy and security. Internal audit must provide assurance	• Consumers' threat of organisations 'leaking' information • Hacking or cyber terrorism	• Data used are more reliable
5	Extensible business reporting (XBRL)	• Standards-based way to communicate business and financial information	• Correct (exact) taxonomy and its mapping to financial information and coding – no mistakes allowed • Protection of documents and data	• Financial information readily available and easier to search • More user friendly in spreadsheets • Accelerate the use of continuous auditing

	Area	Explanation	Threat	Advantage
				• Enhance flow of information and communication between parties • Timely reporting • Automated audit-trails • Access information from remote locations
6	Enterprise resource planning (ERP)	• Integrates all departments and functions onto one computer system, e.g., SAP	• Knowledge of internal auditors of the system • Many changes for organisation need to be monitored	• Standardised systems and processes easier to audit • Centralised data source improves access to data • Real-time data increase timeliness
7	Electronic working papers	• Document the internal audit engagement process electronically	• Limited knowledge of the programs used • Costs involved	• Simplifying management of internal audit function and internal audit engagements • Easy organising, linking and locating between different areas, e.g., from the audit plan, to the evidence, to the audit finding to report writing
8	CAATTs	• Wide range of tools and techniques assisting the internal auditor during the audit engagement/planning activities/ reporting process	• Limited knowledge of products available • Lack skills in using tools and techniques • Costs involved	• Wider coverage of audit scope and procedures freeing internal auditors to focus on critical thinking aspects • Less time consuming • Performing tasks otherwise impossible
9	IT knowledge	• Obtaining, sharing and maintaining relevant information	• Not constantly updating, thus outdated information	• Eliminate duplication

(Source: refer to discussion)

2.6.7 Conclusion

It is clear from the above discussion that there are a few serious threats to the profession. Aspects that should especially be taken note of are the independence of the internal audit function, the required competencies and skills of internal auditors, and the global financial crisis affecting the business environment. However, it is possible to turn some of these threats into advantages for the profession. The global financial crisis as well as the wide scope of current responsibilities could be used to convince management (and chief audit executives) that risk matters are of the utmost importance for the organisation and the way internal auditing performs their duties. IT is a reality and has many advantages and threats for the profession (refer to table 2.6 on p. 128). Where internal auditing is sometimes used by management as an item on the corporate governance checklist, it could be turned around to convince management that internal auditing can add value by eliminating surprises such as the current financial crisis through its contribution to the risk management process. This will, however, only be possible when an organisation has an effective and efficient internal audit function.

2.7 EFFECTIVE AND EFFICIENT INTERNAL AUDIT FUNCTION

From the above discussion, it can be argued that it is vital for organisations to have an internal audit function – being that it is one of the cornerstones of sound corporate governance – and that many institutions such as the JSE Limited and the NYSE have made internal auditing a listing requirement. But to have an effective internal audit function (refer to the King Report quote in section 2.6.1 on p. 113) that contributes to the governance process by adding value is something totally different from just establishing an internal audit function to adhere to sound corporate governance principles. Various writers have identified contributing factors or a strategy to enhance internal auditing's effectiveness. These are briefly listed below (Boyle 2003:1; Gray 2004:19-23,171-173; Harrington 2004:1-2; Spencer Pickett 2004(b):29-30,708-711; ECIIA 2005:29-31; Carcello *et al.* 2005:69-81; Sass 2005:14-18; Corbin 2005:29-31; Krell 2005:20; Oxner & Oxner 2006:51-57; Rittenberg & Anderson 2006:51-54; Mihret & Yismaw 2007:471-481;

Dixon & Goodall 2007:83-87; Ernst & Young 2008:28-31; Robert Half International 2008:3-5; Christopher *et al.* 2009:205-214; IIA 2007(b):9):

- the function's authority or standing within the organisation (including independence – refer to section 2.6.1 on p. 113), including:
  - the relationship with the audit committee;
  - resources entrusted to the activity;
  - the standing of the chief audit executive within the organisation;
  - the suitability and adequacy of the internal audit personnel to perform the duties expected of them;
  - the size and scope of the internal audit function within the organisation;
  - the relationship with the external auditors;
  - the reliance of the external auditors on the work performed by the internal auditors; and
  - the outcome of a quality assurance review on the internal audit function performed either in-house or by external parties;
- the resources available to the function, including:
  - budget adequately funded (for example as % of revenue, assets and/or expenses and compared with the external audit fees);
  - suitable staff for a specific organisation (strategic) or audit engagement (operational) including outsourcing specific needs or expertise;
  - market-related salaries; and
  - up-to-date technology;
- the role of the chief audit executive:
  - involve board of directors, audit committee and human resource department when appointed;
  - suitable qualifications (CA or CIA), skills (accounting, auditing, etc.) and experience (managerial and/or internal auditing);
  - ability to earn the respect of senior management and the audit committee;
  - ability to attract and develop internal audit staff to build a high-quality staff component; and

- best focus to suit the organisation as a whole, including an understanding of the organisation's core strategies;

- the qualities of all internal audit personnel:
  - high level of professional ethics;
  - suitable qualifications (minimum of an undergraduate degree);
  - professional designations;
  - necessary experience;
  - appropriate skills (for example, computer and communication skills);
  - training and development of staff;
  - career development management; and
  - proper communication skills;
- the scope of internal auditing activities within the organisation:
  - budget between 0.03% and 0.2% of annual revenue; and
  - no limitations placed on activities, for example, access to all information, tasks performed as deemed necessary, etc.;
- the quality of internal audit performance:
  - completed audit engagements compared to the internal audit function's plan;
  - length of time to issue audit reports;
  - results form auditee surveys; and
  - performing the audit engagement efficiently and cost-effectively;
- coordination with external auditors:
  - share information, documentation, for example, audit reports; and
  - regular evaluation of coordination (review by audit committee) to minimise cost and increase audit effectiveness; and
- adequate communication including reporting:
  - report engagement findings to level that can provide due consideration;
  - functional reporting to audit committee with executive summary (activity reports) to other relevant senior parties;
  - clear, well-written reports focusing on significant aspects; and
  - other relevant communication including oral reporting, interim reporting, year plan, progress reporting.

It is important to understand that real value-adding by the internal audit function can only occur in a truly effective internal audit function. Corporate governance codes, other guidelines and legislation all include an internal audit function as a prerequisite for sound corporate governance principles. It is not a difficult task to establish such a function and then add a 'tick' to the list of corporate governance requirements. The true value of an internal audit function lies within the fact that it has the freedom to audit as needed with the audit committee providing directions and being the body that enhances the function's independence.

2.8 SUMMARY AND RELEVANCE TO THE STUDY

Many arguments on the evolution of the internal audit profession are debated in this chapter. This section summarises the aspects most relevant to this study, as identified in the literature.

Internal auditing has evolved from the external audit profession, with the IIA being the global governing body and having worldwide representation, including a national institute in SA. When internal auditing and external auditing are compared, many points of contact are identified that substantiate that the two professions do have an influence on each other.

The accountability and agency theories are explained in the context of both these professions, and with regard to this study:

- internal auditing provides additional assurance to the principle (shareholders) that operations are performed effectively and efficiently;
- internal auditing assists the agent (management) in reaching objectives; and
- internal auditing strengthens the accountability theory when reporting crucial aspects to the independent audit committee.

Changes in the internal audit profession were initiated with the issuing of a revised definition in 1999, adding the following:

- consulting activities reflecting on possible assistance to management in accomplishing objectives;
- adding value by facilitating, identifying and even implementing (consulting services) improvements; and
- apart from internal control, the scope of internal auditing expands to incorporate risk management and governance systems.

Although the revised definition has expanded the role of internal auditing to a great extent, other developments have also added to the evolution of the profession, namely:

- from within the profession:
    - a tendency to outsource or co-source the internal audit function or part thereof – with the role that internal auditing has to play in risk management, whether this tendency contributes positively to the profession needs to be investigated;
    - internal auditing needs additional skills sets, with IT and risk management being high on the list of specialisations needed; and
    - the IIA had developed new guidance on these fields, but it seems that it is still insufficient;
- external developments:
    - globalisation and the skills needed for certain specialised fields mean potential challenges for internal auditors, namely the risks related to a global organisation, as well as the effect of the shortage of skills;
    - corporate governance (with internal auditing seen as one of the cornerstones) has developed in the private and public sectors, globally and in SA, with numerous guidance being issued in the form of codes and legislation; and
    - in major corporate scandals, the question was asked – where were the internal auditors?

These factors all contribute to how internal and external stakeholders perceive internal auditing, and this will ultimately affect the way internal auditing is utilised.

With the evolution of the profession, new threats have also emerged. These include the following:

- the status that the internal audit function enjoys is directly linked to its independence from senior management – established by appropriate reporting lines and the amount of consulting services performed for senior management *versus* assurance services performed for the board;
- internal auditing should be more than a 'tick off' of the corporate governance checklist, but should be utilised by management to its fullest advantage;
- the competency, skills and knowledge of internal auditors, the lack thereof being a threat to performing internal audit activities optimally, need to be addressed by the IIA in the form of guidance;
- with senior management expecting more from the internal audit function, the threat of doing more than should be included in the internal audit scope, must be guarded against as it could have an effect on the productiveness of the function;
- the current global financial crisis could affect the profession as follows:
    - less resources available to the internal audit function;
    - the IIA Inc., the global governing body, has fewer resources available to develop new guidance;
    - management is asking for an increase in attention to risk management; and
- technology could be a foe or a friend to internal auditors, being either a driver (providing assurance on IT-related aspects), or an enabler (using IT to assist with performing internal audit activities).

For internal auditing to be really recognised as a force in the corporate governance field in general, and the organisation specifically, the function should be established in such a manner that it is seen as effective and efficient in adding

value and assisting management with the concepts of internal control, risk management and corporate governance.

Internal auditing is an evolving profession with many internal and external factors enforcing the development of the profession. One of these areas that have an enormous influence on the profession is corporate governance, specifically, risk management. These two concepts are discussed in the next chapter.

CHAPTER 3
THE DEVELOPMENT OF CORPORATE GOVERNANCE WITH SPECIFIC REFERENCE TO RISK MANAGEMENT

3.1 INTRODUCTION

In the previous chapter, the evolution of internal auditing has been discussed. Two of the new concepts incorporated into modern internal auditing are corporate governance and risk management. The concept of corporate governance is not new to the business environment, but many new methodologies and developments influencing it have occurred over the last few decades, for example, the evolution of risk management.

In short, corporate governance is about making sure that an organisation is managed properly (IOD 1994:1). For a full discussion on corporate governance principles, refer to the recently published King Committee's Report on Governance (IOD 2009). As the business environment is not static, the directing and controlling that have to take place when managing an organisation also need to adapt to the changing environment. In an ideal situation, corporate governance is thus not a set of rules, but rather a way of thinking that stimulates continuous development and updating in order to address emerging trends (IOD 2009:7). This is, however, not entirely possible for the public sector as it is primarily driven by legislation. Therefore, legislation reflecting sound governance principles is needed for public sector organisations to implement systems and processes that will make sure that they are managed properly.

To address the much-needed guidance on corporate governance, many codes, regulations and legislation have been developed by governments and other influential bodies. These documents are constantly being updated, and in the most recent ones risk management is included as a prominent part of corporate governance strategies.

In terms of corporate governance, there are many parties and other aids that could assist top management in ensuring that their organisation is managed properly. One of these is a formal risk management framework. In today's competitive world it is becoming increasingly difficult for organisations to achieve good results or for government organisations to provide the necessary services in an economical, effective and efficient manner (SA – Public Service Commission 2003:4; COSO 2004:3; IFAC 2004:13; Merna & Al-Thani 2005:2). The reason for this is, amongst others, that the growing globalisation of the market in which organisations operate brings about greater opportunities, but also increased complexity and constant change. This causes greater potential for things to go wrong, or in a business environment, risks threatening the organisation reaching its objectives. But it is also true that no organisation can thrive without taking risks. Therefore, as risk, and in particular business risk, is part of every organisation, it has to be managed to ensure that organisations can still achieve their objectives.

In this chapter, the development of corporate governance in general, and more specifically risk management, is discussed. The need for risk management, global guidelines as well as SA developments for both the private and the public sector, and the responsibilities of certain parties are discussed. Thereafter, the concept of risk management is scrutinised to understand what is meant by risk within risk management, the risk management process and the maturity of the risk management framework. Lastly, the future of risk management is investigated by studying current trends, weaknesses, successes and new developments.

3.2 CORPORATE GOVENANCE

In this section the concept of corporate governance is introduced with brief reference to its history and development. Corporate governance is a very wide concept and it is therefore difficult, and perhaps impossible, to fit it into one specific definition. There is no formal definition that can be applied to all users – as such, by evaluating discussions and methodologies, a list of common factors is drafted to try and explain the term. The need for and value of a sound

corporate governance framework is investigated, identifying the accountability of management as one of the crucial elements in the foundation of corporate governance.

3.2.1 Introduction to corporate governance

Corporate governance has been practised for as long as trading activities have been taking place. In 1776 (cited in Tricker 2000) Adam Smith concluded that directors of companies are the managers of other peoples' money and, therefore, will most probably not watch over it as if it were their own – referring to corporate governance principles. Since very early times, greedy and unscrupulous individuals were trading at the expense of stakeholders such as customers, employers, communities, etc. Governments and other bodies reacted to this situation by introducing sets of rules, legislation and codes to curb this unacceptable behaviour of abusing the free market system. During the twentieth century publicly-held organisations became a common business form resulting in even more stakeholders being affected by the decisions of the organisation (Tricker 2000; Solomon 2007:2-5).

The growing concern for proper governance has its roots in the demand and expectations of society (Spencer Pickett 2004(a):24; Solomon 2007:7). Organisations are managed on behalf of people who have some form of stake in the organisation and who would like to see a return on their investment, sustainable growth, or meeting of service delivery expectations. At the same time, management has certain performance targets to meet. The underlying theories for this problem are (IOD 2002:11-12; Solomon 2007:17-30,143-150; Mallin 2007:12-16; Letza, Kirkbride, Sun & Smallman 2008:17-32; Abdullah & Valentine 2009:89-93):

- Accountability theory – directors are accountable to all stakeholders on the governance of the organisation (refer to sections 2.3.3 on p. 68 and 3.2.4 on p. 150 for a detailed discussion).

- Agency theory – based on the principle that investors delegate to directors their mandate to manage the organisation.
- Class hegemony theory – the directors regard themselves as the top elite group of the organisation, thus when appointing a director, consideration must be given to how well the individual will serve the organisation.
- Managerial hegemony theory – the influence of directors could be weakened by senior management overruling the board's decisions (refer to sections 2.4.1.1 on p. 71 and 2.6.1 on p. 113 for a discussion on the assurance *versus* consulting services of the internal audit function as an example of this theory).
- Political theory – developing shareholders' voting support rather than purchasing voting power with regard to the government's support.
- Resource dependency theory – providing access to resources needed by the organisation.
- Stakeholders theory – focusing on stakeholders' interests provides for representation.
- Stewardship theory – the directors of the organisation are regarded as the stewards of its assets and will act in the best interest of all.
- Transaction cost economics theory – the appropriateness of the governance structure assisting the organisation's transactions – thus the theory is based on the combination of individuals within the organisation that arranges transactions to meet their interest.

The task of successfully matching management's performance targets with stakeholders' expectations can be enhanced by implementing sound corporate governance principles (Hermanson & Rittenberg 2003:28). Various parties acknowledge the need for proper guidance in this regard, for example, many countries and other bodies have provided and are still in the process of providing guidance by publishing codes and reports such as SA's three King reports (principles-driven or 'apply/comply or explain'-principle), as well as legislation such as the USA's SOX (rules-driven or 'comply or else'-principle) on this concept (refer to sections 1.3.1 on p. 13 and 1.3.2 on p. 14 for a brief discussion on these).

In the early 1980s (Fama & Jensen 1983:11) corporate governance was defined by mainstream accounting and finance literature as the range of control mechanisms that protect and enhance the interests of business organisations' shareholders. Scientific research on modern corporate governance principles was first published in 1983 (Tricker 2000). In 1984, Professor Bob Tricker of the University of Hong Kong Business School, an individual widely recognised for his role in developing corporate governance principles (OECD 1999), concluded that management is about running a business and corporate governance is about seeing that it is run properly (Tricker 2000). The UK's Cadbury Report on corporate governance added to this description that there should be a balance between economic and social goals, thus between the interests of individuals, society and organisations (Cadbury Report 1992). The first King Report broadened this theory and incorporated the stakeholder-link, including shareholders, contractual stakeholders and non-contractual stakeholders – being the community, customers, employees or suppliers (IOD 1994:23). The OECD (1999) added that sound corporate governance is a structure through which the objectives of the organisation are set and performance is monitored.

From the above discussion, although at first glance it seems that corporate governance is a simple concept, the implementation thereof within an organisation is a complex matter. Corporate governance is a comprehensive term that cannot be reduced to one definition. The two main parties involved, namely the ones that 'want' something (for example, the shareholders and general public) and the ones that have to 'produce' something (for example, management and government) must work towards a common goal for an organisation to reach its full potential. Guidance is essential to ensure that this is achieved.

3.2.2 The definition of corporate governance

The word governance derives from the Latin word *gubernare,* which means steer and refers to the steering of a ship (Tricker 2000; Solomon 2007:12). This implies that governance is related to the direction rather than the controlling of something, in this case – organisations.

Many definitions and descriptions have tried to explain the concept of corporate governance. Some of the most widely recognised are the following (listed according to publishing date):

> …corporate governance mainly involves the establishment of structures and processes, with appropriate checks and balances that enable directors to discharge their legal responsibilities, and oversee compliance… (IOD 2009:8).

> …the system of checks and balances, both internal and external to companies, which ensures that companies discharge their accountability to all their stakeholders and act in a socially responsible way in all areas of their business activity (Solomon 2007:14).

> Corporate governance is the interaction of a company's management, its board [of] directors, and its shareholders to direct and control the firm, and to ensure that all financial stakeholders (shareholders and creditors) receive their fair share of the company's earnings and assets (Standard & Poor's cited in Dallas 2004:21).

> Corporate governance is essentially about leadership (IOD 2002:19).

> Corporate governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation's resources are used responsibly (Information System Audit and Control Foundation 2001 – this definition is also recognised by IFAC 2004:9).

> Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of

attaining those objectives and monitoring performance are determined (OECD 1999:11).

Corporate governance is simply the system by which companies are directed and controlled (IOD 1994:1).

The country's economy depends on the drive and efficiency of its companies. Thus the effectiveness with which their boards discharge their responsibilities determines Britain's competitive position. They must be free to drive their companies forward, but exercise that freedom within a framework of effective accountability. This is the essence of any systems of corporate governance (Cadbury Report 1992:par1.1).

Corporate governance is the system by which companies are directed and controlled (Cadbury Report 1992:par 2.5).

The above can be summarised as follows:

- Corporate governance is a process(es) and/or system(s) that consists of checks and balances, operating within a framework or structure.
- It includes, but is not limited to financial aspects.
- Management develops a unique structure that will suit its organisation's needs.
- The structure is developed in such a manner that it strives to lead by means of directing rather than controlling (refer to section 3.2.3.3 on p. 149).
- Corporate governance is about leadership and therefore the board of directors and executive management are responsible for driving these processes and systems.
- Organisations are accountable to a comprehensive network of stakeholders (refer to section 3.2.4 on p. 150).

- All parties, such as the board, senior management, other employees, shareholders, etc., have a role to play and have certain responsibilities to fulfil.
- The board's responsibilities include:
  - providing strategic direction;
  - ensuring that objectives are achieved;
  - ascertaining that risks are managed appropriately (refer to section 3.3 on p. 153); and
  - verifying that the organisation's resources are used responsibly.
- All the parties involved (management, board, shareholders, society and other stakeholders) must work together to obtain the best results. There is thus not a fixed structure that will suit all organisations.

The above sketches a broad picture of what is understood by the term corporate governance. However, new developments within the world at large could have a direct influence on how organisations should be managed, beyond the obvious. For example, although a specific organisation may have a limited exposure to environmental concerns, it will nevertheless be affected by the consequences thereof and thus needs to address the potential impact sooner rather than later. The third King Report (IOD 2009:10-11) identifies leadership and sustainability as core principles for any corporate governance guidance. Leadership is included as leaders are the catalysts for change and guide the effective responses of the other stakeholders. Without effective leadership, the organisation cannot achieve sustainable, social and environmental performance. Sustainability is included as nature, society and business are interconnected with one another and need to be understood and managed accordingly.

These definitions and the discussion thereof mainly focus on definitions developed for the private sector. As this study incorporates both the private and the public sectors (refer to section 1.5 on p. 24), corporate governance from the public sector's perspective must be investigated. It is important to note that corporate governance is primarily built on principles (refer to the King reports) and these are applicable to all sectors. Therefore, although terminology may

differ, the application of the principles should be consistent. According to the literature (USA – Agency for International Development 1998; Du Toit *et al.* 2002:64; Halachmi 2005:302; Van der Waldt & Du Toit 2005:46), corporate governance in the public sector can be summarised as the ability of a government (management) to develop a public management process (framework or structure) that ensures that the country's citizens' money is spent wisely (obtaining the best results) to enable maximum service delivery. It is obvious, when comparing this summary of corporate governance to the one on pp. 143-144, that the concept of governance is applicable to both the private and the public sectors.

Although it can be concluded that corporate governance has developed over the years and is a recognised concept that must be incorporated in private sector and public sector organisations, the question remains whether there is a need for it in modern society. Secondly, is there a need for all the new guidance developed on an on-going basis? For example, in SA over the last fifteen years three corporate governance reports have been written ranging from a mere fifty three pages for the first King Report (IOD 1994), to a hundred and thirty five pages for the last document (IOD 2009). Does the first report not provide enough guidance as it is a principle-driven document? A further concern with regard to corporate governance is the fact that organisations may treat it as a list of 'must do's' instead of implementing a new way of thinking to improve current practices (refer to section 2.6.2 on p. 117 for a discussion on internal auditing as one of these elements on the list). On the positive side, many codes refer to a 'comply/apply or explain' concept (refer to section 3.2.3.3 on p. 149) that is purely principle-driven and more widely accepted by boards. This chapter will contribute in trying to answer the above-mentioned questions with specific reference to risk management.

3.2.3 Factors influencing the need for and value of new developments

Many factors have contributed to the development of corporate governance, with the separation of management from ownership contributing the most. Other factors include the increase in litigation with shareholders of failed organisations

seeking compensation, the increase in corporate and government scandals, the growth in the number of major corporations (corporate giants) and in investor power, the lack of leadership from governments and lastly the business environment's response to all this, namely corporate codes and legislation (Tricker 2000; Hermanson & Rittenberg 2003:38-40; Spencer Pickett 2003:27-45; O'Brien 2005; Dimma 2006:13-22; Lubbe 2009). Three of these factors that have influenced the business environment the most over the last decade are discussed briefly.

3.2.3.1 Corporate scandals

In section 1.3.4 on p. 17, corporate scandals are discussed, with specific reference to the two most well-known scandals that occurred in the 2000s, namely Enron and WorldCom. It is well-known that the USA government reacted to these scandals by promulgating corporate governance legislation, namely SOX (USA – 2002), which has had far reaching consequences for the USA as well as other countries dealing with USA organisations (refer to section 3.2.3.3 on p. 149 for a discussion). The questions to be answered are whether organisations where corporate scandals occurred had proper corporate governance principles in place, and if so, why these did not prevent the scandals from occurring.

According to a study performed by Mardjono (2005:273-274), Enron and HIH Insurance (Australia) did not fail because they were doing bad business or not recognising good governance principles, but because they used the governance framework as a tool to keep investors happy. This fact is supported by Solomon (2007:42-46) when reflecting on the collapse of Enron and Parmalat. It seems likely that corporate governance principles were implemented and 'ticked off' (refer to section 2.6.2 on p. 117) instead of the essence of the guidance being inculcated with the right attitude. The International Federation of Accountants (IFAC 2004) launched a project where the causes of twenty seven corporate failures were explored against a governance framework. Failures could be linked to the following key aspects (IFAC 2004:14-17):

- culture and tone at the top fostering unethical behaviour through example and standard setting;
- dominant and charismatic chief executives;
- the board of directors failing to fulfil oversight duties over chief executives; and
- weak internal control system, for example, a lack of proper segregation of duties in the higher ranks of the organisation.

These aspects all refer to the attitude with which corporate governance principles are implemented as opposed to simply following the letter of the stipulation. It could thus be concluded that although an organisation has all the necessary systems and processes in place to proclaim that it has a sound corporate governance framework, if the framework is used as a checklist instead of a tool to truly assist in improving the organisation as a whole, scandals will keep on occurring.

3.2.3.2 Investors' requirements

The growth in the number of corporate organisations in contrast to privately owned organisations, the number and size of corporate giants, the complexity of the business environment, and more specifically, trading markets, all contribute to investors being more careful when investing (Dallas 2004:5-6; Hodge 2004:15-16; Markham 2006:547; King 2007; Solomon 2007:109-116). Whether sound corporate governance principles implemented by an organisation will affect an investor's decision when making an investment is debatable. Studies reveal contradictory evidence.

On the one hand, studies amongst investors (McKinsey (2002) and Standard & Poor's (2002) cited in Wilkes 2004:13-15; Ernst & Young 2006:10-11; Diamond & Verrecchia (1991), Kim & Verrecchia (1994), Healy (1999) and Kothari (2001) cited in Solomon 2007:146-147; Deutsche Bank (2002) cited in Marx 2008:67) reveal that the market does reward good corporate governance. Results indicate that investors are willing to pay a premium of between 12% in North America and

up to 30% in developing countries on organisations revealing sound governance principles. In a study performed by Alexakis *et al.* (2006:682-683) on the effect of corporate governance legislation on the mean returns and price volatility of organisations, it is concluded that although it was possible that other factors could also have contributed to the positive impact observed, corporate governance legislation definitely played a role.

On the neutral side, according to a study performed in Poland (Aluchna 2009:185-198) on the effect of corporate governance on corporate performance, a negative correlation was obtained during the first year of implementing sound governance principles, easing out towards the third year, with no remarkable difference overall. This could imply that the implementation of corporate governance costs organisations money, and although the initial implementation's cost is phased out fairly soon, the true value of following a governance framework will only be realised after a few years. Additionally, the study's results should be viewed cautiously taking into consideration that Poland was ruled until recently by a communist government where corporate governance principles were most probably not strongly supported.

One way of assisting investors in determining the corporate governance effectiveness of an organisation is to use a rating system (Dallas 2004:5-6). Studies (Heracleous 2001:165; Hermanson 2004:37; Donker & Zahir 2008:92) indicate that although many such systems exist, the link between the organisation's performance and the rating score is weak, with reasons varying from corporate governance best practices (theoretical) being irrelevant to the outcome of the organisation's performance (practical), to different types of organisation requiring different types of guidance. This boils down to the fact that although corporate governance guidelines are very effective tools to assist management in managing the organisation, their true value lies within good corporate governance and not good corporate governance ratings. Management still has to produce the results and merely adhering to a checklist of governance requirements is not going to produce the results.

3.2.3.3 Principles-driven (codes) *versus* rules-driven (legislation) guidance

The debate about whether corporate governance should be rules-driven or principles-driven is an on-going one (IOD 2009:6-7). According to Markham (2006:662), the USA government was convinced that, after numerous corporate scandals, a rules-driven guidance was needed to regain the public's trust, stabilise the markets and normalise the business environment. He argues that new laws, for example, SOX (USA – 2002) are promulgated after each major scandal, attacking aspects of corporate governance, but the perpetrators are either in jail or have fled the country, and the innocent are punished with new rules and regulations. This is echoed by Chambers (cited in Jackson 2004:59), a director at an audit consulting company in the UK, as well as Dallas (2004:23-24), the managing director of Standard & Poor's in the USA. Both argue that a rules-based approach alone is inadequate. Governments are passing more legislation to counter loopholes in the law – other players are simply finding new loopholes.

Influential people like Mervyn King, chairman of the King Committee in SA, are not convinced that a rules-driven approach is a long-term solution. King (Barrier 2003:71) states that principles are more effective than rules by arguing that running a business is not a simple matter and those who manage it do not have the vision to foresee what will happen on a day-to-day basis. They need the flexibility to manage their business as situations change. Legislation is too rigid and does not complement this fact. The recently issued third King Report on Governance (2009:7) goes even further and refers to an 'apply or explain' approach, the second report merely referred to a 'comply or explain' principle (Deloitte 2009; Ernst & Young 2009(c)).

Furthermore, the rules-based approach is a 'one size fits all' approach. This could hamper the tasks of other role players and money could be channelled into areas where no or little improvement is possible. For example, internal auditors could be so tied up struggling to provide assurance on all the legal requirements that it prevents them from adding value in other areas, such as assisting management in identifying and managing crucial risks. According to the third King Report (IOD

2009:6) the cost for organisations to comply with SOX since 2002 is more than the total write-off that occurred during the Enron, WorldCom and Tyco corporate scandals combined; thus organisations are pouring money into compliance with rules when some of those rules could actually be irrelevant in preventing fraud for a specific organisation.

Many countries in the Commonwealth, including SA, as well as in the European Union have adopted the principles-driven approach (Solomon 2007:50-51; IOD 2009:6). With this approach, much emphasis is placed on the duties and leadership of the board, which should act in good faith in the best interests of the organisation and all its stakeholders. For the other stakeholders to be sure that management is performing their duties to the best of their capabilities, proper accountability is of the utmost importance.

3.2.4 Accountability as an element of corporate governance

As discussed in section 3.2.1 on p. 139, accountability is one of the underlying theories of good governance (Grant & Keohane 2005:29; Solomon 2007:143; Mallin 2007:12; Brennan & Solomon 2008:885-906; Porter 2009:156-182). Although all the underlying theories of corporate governance are important, accountability is highlighted due to the fact that internal auditing plays a significant part in this theory (refer to section 2.3 on p. 63 and more specifically figure 2.1 on p. 69). According to Gloeck (2005/6:15-17), even if an organisation obtains high scores for sound corporate governance practices, questions should still be asked as to whether the systems and structures are transparent, the processes used are inclusive, fair and equitable, and whether the organisation is accountable or answerable to various related parties. This is echoed by Standard & Poor's managing director where he argues that the quality and scope of an organisation's accountability and disclosure are fundamental concerns for investors (Dallas 2004:87).

To be able to produce the results demanded by the stakeholders, management has to delegate certain responsibilities to subordinates. These subordinates receive the responsibility to ensure that a task is executed in accordance with

certain criteria and that objectives are achieved. Accountability entails the duty of these subordinates and their management to report to the stakeholders that the responsibility has been fulfilled, as well as the manner in which the task was performed (SA – Public Service and Administration 2003:64; Curristine 2005:137-138; Solomon 2007:146). This can be achieved by either implementing a proper reporting process, or having a transparent governing system, or through implementing both.

Studies performed by Ernst & Young (2006:10-11), Porter (2009:156) and Eccles, Pillay and De Jongh (2009:21-38) argue that although the discharge of corporate accountability traditionally relied on the preparation, independent auditing and distribution of the financial statements and related reports, this has now changed due to many new developments such as major corporate failures (refer to section 3.2.3.1 on p. 146) and investors' increased demands (refer to section 3.2.3.2 on p. 147). Stakeholders demand more comprehensive accountability on corporate governance aspects.

For the private sector accountability refers to the management team being accountable to various stakeholders (for example, shareholders, employees, lenders and suppliers) as well as potential stakeholders (for example, investors) for spending the resources of the organisation wisely (Sherer & Kent 1983:1). Although the accountability theory is well established in the private sector (Loots 1989:2-4; Solomon 2007:144-150) with numerous reports being issued by management for the benefit of various stakeholders and the independent external auditors performing audits on the financial statements and reporting to stakeholders, over the last few years much has been written on the expectation gap between what stakeholders expect to be performed by the external auditor and what is actually done. This indicates a potential weakness in the accountability theory (Gloeck & De Jager 1993; Koh & Woo 1998:147; Sidani 2007:288). Furthermore, studies indicate that shareholders and potential investors are becoming more demanding, asking for timelier and broader disclosure (McKinsey cited in Wilkes 2004:13) and more information on non-financial aspects (Standard & Poor's cited in Wilkes 2004:14).

In the public sector, management is accountable for how resources are spent (Pauw *et al.* 2002:29,136-137; Du Toit *et al.* 2002:219; Wikipedia n.d.(c)), both to external parties (for example, the taxpayers) and internal parties (for example, to supervisors, directors and boards). Governments are facing increasing accountability demands. On the one hand citizens expect better quality and higher quantity service delivery, and on the other hand they want to pay less taxes (Curristine 2005:127). The citizens of a country demand to know how their tax money is spent. For SA citizens, financial statements issued by a government organisation and the accompanying audit reports issued by the Auditor General are the most comprehensive and reliable reflection of accountability in the public sector. However, in practice, the successful application of the accountability theory is debatable. According to Lubbe (2008(a):28-29) the number of qualified audit reports in the public sector in SA is an indication of the state of financial reporting and the poor state of government organisations, and is also a reflection of the lack of proper accountability in the SA government. Global research (Palmer 2008:265-285) supports this statement by adding that government audit reports are not always perceived as being trustworthy due to the fact that many factors such as the media, personal political preference and prior expectation causes bias in the audit process, reflecting in the audit report. Lastly, linking accountability to risk management, according to a public sector forum, Transforming Bureaucratic Cultures in the USA (Potok 2009), managing internal and external risks is one of the main elements in accountability challenges and needs to be incorporated in all government organisations.

3.2.5 Conclusion

Corporate governance, although not a new concept, has developed greatly over the last few decades. Factors influencing this tendency include the increase in corporate scandals, investors being more demanding, and the move from a rule-driven to a more principle-driven management style that compliments corporate governance principles. Still, the question remains whether there is a need for corporate governance and related guidance. Many organisations treat sound governance principles as a list of requirements instead of a way to direct activities – thus not performing corporate governance requirements with the right attitude.

However, said that, management is accountable to their stakeholders regarding how they steer the organisations' resources. Corporate governance, including risk management, when viewed with the right attitude, is an excellent concept to assist them with this requirement.

3.3 RISK MANAGEMENT AS PART OF CORPORATE GOVERNANCE

Formalised risk management frameworks have been recognised by many as an effective tool in assisting management with corporate governance. This is evident from the following statement made by US President John F. Kennedy in the 1960s (IIA 2009(c)):

> There are risks and costs to a program of action. But they are far less than the long-range risks and costs of comfortable inaction.

More recently, this is supported by the fact that risk management is included in most corporate governance codes and legislation (refer to table 3.1 on p. 164). In short, risk management is a framework adopted by the board on how to manage risks threatening the reaching of the organisation's objectives.

In this section risk management is briefly introduced and some of the prominent corporate governance guidelines and other literature on risk management are scrutinised to try and provide common factors for a formal definition of risk management. Thereafter the reason why risk management plays such a prominent role in organisations, as well as global and SA guidelines and developments are discussed. Lastly, the parties involved with risk management and their roles and responsibilities are briefly mentioned.

3.3.1 Introduction to risk management

The idea of the measurement of the chance of an outcome, the ability to define what may happen in the future, as well as the means to manage the outcome of chances and the future by identifying alternatives and choosing the best suitable one, dates back at least 2000 years (Bernstein 1996:2-4; Merna & Al-Thani 2005:3-9; Spencer Pickett 2005:1-4). The rise of the insurance business was the first formal risk management technique and dates back to the early 1700s (Merna

& Al-Thani 2005:31-32). Not all risks are insurable, and in the 1970s, project risk management developed to include quantitative risk assessment, including risk methodologies and processes (Archibald & Lichtenberg 1992:83-84). During the 1980s (Merna & Al-Thani 2005:32-33), much development took place on risk management including formalising methodologies. In the 1990s (Merna & Al-Thani 2005:33-34), risk management became a formal process that management could use to assist them in managing the taking of chances and identifying possible future events that could have an effect on the organisation.

The root of modern risk management theories lies in the ultimate objective of management to maximise shareholders' value (Meulbroek 2002:5) or, for the public sector, the responsibility of government to protect the citizens of the country by maintaining order, defend the country against attacks and ensure harmony amongst business and/or individuals (Kalaw 2002; UK – Cabinet Office 2002(a):4). Atkins and Webb (2005:26) argue that the nature, fundamentals and consequences of risk for a profit-driven and non-profit organisation are exactly the same; the first measure risks in financial returns whereas the latter measure risks in the threat of achieving quality objectives. Therefore, the argument of Handy (1999) that risk management should not be seen as a separate form of managerial activities, as it includes elements such as predicting, planning, prevention and reaction, holds for both the private and the public sector, as these elements occur in both.

As indicated above, the development of a formal risk management process and the evolution of a more comprehensive risk management framework during the 1990s and beyond, highlighted the fact that risk can be managed by using a structured and systematic approach and by adopting certain structures and frameworks within the organisation.

Since the 1990s, risk management has evolved with such speed, as reflected in the various corporate governance codes and other guidelines (refer to sections 3.3.4 on p. 163 and 3.3.5 on p. 173), that the questions that ought to be asked are, *inter alia*, whether the growth was not too fast, whether the best possible methods have been developed and are being used, have the board succeeded in

'selling' this new concept to all the stakeholders, and whether all the relevant individuals are optimising risk management for the benefit of the organisation. In the rest of this section, the concept of risk management from a corporate governance perspective, the increasing importance of risk management as illustrated by its inclusion in corporate governance codes and legislation, as well as the most relevant role players' responsibilities are debated to try and provide some of these answers.

3.3.2 The definition of risk management

Like corporate governance, risk management is not an easy concept to define. It consists of two different words each having a significant effect on the total, namely risk (refer to section 3.4 on p. 182 for a detailed discussion) and management (referring to planning, organising, directing and controlling the activities within an organisation). It is therefore understandable that various definitions and explanations of the term exist, all trying to define the concept.

Although not formally defined or acknowledged, for the purpose of this study, two terms are used to describe the overall risk management concept (these are also preferred by risk experts such as Dr Sean De la Rosa (2008(b)), Alexandra Psica (2008:53) and Deloitte (2009), as well as risk management guidance from the UK government (UK – Cabinet Office 2002(b):9-10), the Australian and New Zealand Standards Board (AS/NZS 2004:5), and the IIA (France) (2005)), namely:

- A risk management framework – the totality of the structures, processes, systems, methodology, individuals involved, etc., that an organisation uses to implement its risk management strategy.
- The risk management process – the process that is used by management to identify, assess, treat, monitor and report risks. This is usually a structured and systematic set of tasks.

A further concept that needs to be clarified before the risk management definitions can be explored, is the scope or extent of the implementation of risk

management within the organisation. This can be explained by referring to the following two terms, namely (Spencer Pickett 2003:132,154; Nocco & Stulz 2006:8-10; De la Rosa 2008(b)):

- Risk management – refers to the dynamic process and other structures in place to identify and deal with risks that impact certain objectives on a micro-level, usually within a silo. For example, it will only focus on a business unit, such as the human resources department or a business process, such as production, and is mostly, but not always, limited to operational-level objectives.
- Enterprise risk management – refers to the extension of risk management across the organisation on a macro-level by integrating all the risk management initiatives including strategic and operational levels (holistic view). Goals with such a framework include, *inter alia*, the:
    - assessment of risk management capabilities including the elimination of duplication;
    - development of a common understanding of risk across multiple units and processes;
    - provision of assurance to the board that strategic objectives will be met;
    - provision of a competitive advantage; and
    - efficient allocation of capital.

The discussion of the definition of risk management includes references to the risk management framework and to the risk management process, as well as both risk management and enterprise risk management. It should also be noted that these four concepts, or parts thereof, are in most cases intertwined in a specific definition. Some of the most frequently used or widely recognised definitions include the following (listed according to publishing date):

> Risk management is the identification and evaluation of actual and potential risk areas as they pertain to the company as a total entity, followed by a process of either avoidance, termination, transfer, tolerance (acceptance), exploitation, or mitigation (treatment) of each

risk, or a response that is a combination or integration [of these] (IOD 2009:123).

The risk management process entails the planning, arranging and controlling of activities and resources to minimise the negative impacts of all risks to levels that can be tolerated by stakeholders whom the board has identified as relevant to the business of the company, as well as to optimise the opportunities, or positive impacts, of all risks (IOD 2009:123).

Risk management is a process to identify, assess, manage and control potential events and situations to provide reasonable assurance regarding the achievement of the organisation's objectives (IIA 2009(a):41).

Risk management is a managerial function aimed at protecting the organisation, its people, assets and profits against the physical and financial consequences of risk (Valsamakis *et al.* 2005:2).

Enterprise risk management is the process by which organisations identify, assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organisation's short and long term value to its shareholders (Casualty Actuarial Society cited in Valsamakis *et al.* 2005:79).

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO 2004:2).

The risk management process is the systematic application of management policies, procedures and practices to the task of

communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risks (AS/NZS 2004:5).

Enterprise-wide risk management is a structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives (IIA 2004:1).

Risk management can be defined as the identification and evaluation of actual and potential risk areas as they pertain to the company as a total entity, followed by a process of either termination, transfer, acceptance (tolerance) or mitigation of each risk (IOD 2002:73).

Enterprise risk management looks beyond traditional hazards and financial risks to the more significant but often ambiguous operational and strategic risks; [*sic*] recognising that good risk management can create competitive advantage and improve shareholder value (UK – Cabinet Office 2002(b):9).

It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities (IRM 2002:2).

Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk aspects (Canada – Treasury Board of Canada Secretariat 2001).

The above definitions can be summarised as follows (also refer to analyses in Merna & Al-Thani 2005:35 and Prinsloo 2008:210-211):

- Risk management is a systematic, consistent and structured framework with a set of actions undertaken, including a risk management process (refer to section 3.5 on p. 191).
- It should be applied continuously as new risks emerge on a daily basis. The risk management framework should thus be reviewed on a regular basis.
- It cuts across the whole organisation (also referred to as enterprise risk management) including strategic as well as operational activities and should be embedded in the day-to-day activities of the organisation (refer to section 3.7.1.2 on p. 217).
- Tasks with regard to actual and potential risks within the risk management process include:
    - identifying risks according to their influence on the organisation's objectives, being either strategic or operational (refer to sections 3.5.2.1 on p. 195 and 3.5.2.2 on p. 196);
    - analysing and assessing these risks (refer to section 3.5.2.3 on p. 198);
    - generating a structured response for managing risks by either eliminating, mitigating (control or share) or accepting them (refer to section 3.5.2.4 on p. 201);
    - (by implication) identifying the cause as well as the source of the risk to ensure that the response will address the risk;
    - restricting risks within the boundaries of risk appetite (refer to section 3.5.2.3.1 on p. 200);
    - communicating or reporting to various stakeholders on the process (refer to section 3.5.2.5 on p. 202); and
    - continuously monitoring and reviewing risks (refer to section 3.5.2.6 on p. 202).
- The objectives of risk management include:
    - providing reasonable assurance that the organisation's objectives will be achieved;
    - enhancing a competitive advantage;
    - protecting all the stakeholders against risks; and
    - maximising shareholders value.

- Various parties are involved, but it is a managerial function, making management responsible for establishing the most appropriate framework and process for the organisation (refer to section 3.3.6 on p. 177).

The above summary provides a logical explanation of risk management. Risk management is, however, not such a simple concept, the reason being that all frameworks consist of, *inter alia*, policies, procedures and practices (activities), and these will differ from one organisation to another. Organisations will thus have to determine the quality and the quantity of activities implemented to determine whether risks are appropriately managed according to the wishes of its board of directors and senior management, and that the risk management is in line with what is communicated to its stakeholders. This refers to the risk maturity of the organisation. The more relevant activities and elements of the risk management framework management have implemented effectively, the more risk mature the organisation is (refer to section 3.6 on p. 205 for a detailed discussion). One organisation could strive to be completely risk mature whereas another may only aim for a 70% maturity level – both being effective for the specific organisation in reaching the objectives of sound risk management.

3.3.3 Motivation for effective risk management

The main reason why risk management has become a necessity rather than a luxury is the increase in the number of risks organisations are exposed to (Bernstein 1996:213; IOD 2002:73; McCarthy & Flynn 2004:4-5; Beasley, Branson & Hancock 2008:45). According to the UK's former Prime Minister, Mr Tony Blair (UK – Cabinet Office 2002(a)), it is not possible for governments to eliminate all risks – both because of the speed with which our environment changes (business, social, technological, etc.) and because people are more aware of and emphasise risks more. Bodies responsible for corporate governance guidelines and legislation are acknowledging this fact with more and more corporate governance guidelines enhancing the importance of risk management (refer to section 3.3.4 on p. 163). Studies (Kleffner, Lee & McGannon 2003:66; Drew *et al.* 2006:127) indicate that this guidance affects the board and its committees – they are becoming more focused on risk

management, more aware of potential risks and are using the risk management framework more and more. Still, organisations could 'tick off' the requirement by implementing some form of risk management system instead of implementing an effective risk management framework. In order for a board, as the party responsible for the oversight of risk management, to decide whether or not to implement a comprehensive risk management framework, the advantages and disadvantages should be measured and compared. If the board, and to a lesser extent, senior management (refer to section 3.3.6.1 on p. 177), are not convinced that risk management is adding value to sound corporate governance principles, an effective risk management framework would most probably not be implemented.

In theory, risk management should have numerous benefits with the only obstacle being the cost aspect. Some of the most important benefits of implementing a structured and comprehensive risk management framework are briefly discussed (Canada – Treasury Board of Canada Secretariat 2001:1; Hahn & Kleiner 2002:1; MORI Social Research Institute 2002; Kleffner *et al.* 2003:65-66; Drew *et al.* 2006:127; Beasley *et al.* 2008:47; Storey 2009:42; Galloway & Funston n.d.:23).

The most prominent benefit of having an effective risk management framework in place is the coordination of all risk management efforts within the organisation. A holistic and consistent approach results in lower costs and increased communication regarding risk across the organisation. Large losses can more easily be avoided by allowing the board and senior management to make more risk-intelligent decisions on the strategic level. Furthermore, as basic processes are effectively managed at low risks and low costs, management can more easily take business and strategic risks for the benefit of the organisation (opportunity risks).

A second benefit is the alignment of all employees in using the same terminology and methodology, thus streamlining the risk philosophy. This could result in employees being less reluctant to buy into the risk management process and, therefore, more likely to provide assistance. It is not always possible or cost-effective to eliminate risks completely. Therefore, there should be a balance

between the cost to mitigate the risk, and the cost of accepting the risk. Although the risk manager or risk department should be equipped to perform the task of balancing risks holistically, line managers and even other employees usually understand the risks facing their division or process the best and this should be taken into account in the framework.

Thirdly, risks can be managed on a proactive basis instead of reactively. The risk management process should be developed in such a manner that risks, arising from change that is constantly affecting the organisation, as well as other emerging risks that could have an effect on the organisation, should be identified, assessed and managed to the benefit of the organisation as a whole.

In the fourth place, the incorporation of an effective risk management process has a positive effect on investors and business performance. One of the biggest rating agencies in the USA, Standard & Poor's, has restructured their rating criteria to incorporate risk management (Moody 2006:40). Studies indicate that the implementation of an effective risk management framework does influence the decisions of investors on a positive way (Ernst & Young 2006:11; Standard & Poor's cited in Puccia 2007; Lam 2009:24). The RIMS maturity model (refer to table 3.5 on p. 209) was used to evaluate 564 organisations' risk maturity against performance. The results indicate that 93% of the respondents' organisations with higher risk maturity levels made better risk-informed decisions and obtained higher credit ratings and lower cost of capital (cited in Minsky 2009). This fact was supported by a study performed by the Association of Insurance and Risk Managers (AIRMIC) based on five case studies of large organisations (cited in Continuity Central 2008).

The risk management discipline, especially enterprise risk management that cuts across the whole organisation, is still a new discipline, and the question remains how the board would know whether their risk management framework is effective for their specific needs. Currently, the lack of negative events is used by many organisations (Lam 2009:26; Galloway & Funston n.d.:22) as the measurement tool to determine whether risk management is achieving its goals. However, this is not sufficient as a major risk could destroy the organisation. Therefore,

organisations should establish performance metrics and feedback procedures to ensure that risk management is doing what it is intended to do, namely identifying and mitigating major and/or critical risks. This strategy should deliver value in the short term – within two to three years at the most. If even more is required to further the reaching of objectives, the strategy could be adapted to also manage low to medium risks. The strategy for implementing and managing the framework will differ from one organisation to another, but certain basic characteristics and elements should always be present for risk management to be successful. Some of the most prominent are discussed throughout this chapter.

3.3.4 Corporate governance guidelines and regulations influencing risk management

As discussed in sections 2.5.2.1 on p. 90 and 2.5.2.2 on p. 92, much guidance has been developed for corporate governance in general. Whether risk management is included in this guidance is another matter. This section first investigates some of the more prominent global documents either mentioning risk management as a corporate governance requirement, or providing comprehensive guidance on, and standards for the topic. Secondly, the developments within an SA context, both for the private and the public sector, are investigated in more depth.

3.3.4.1 Global guidelines

Table 3.1 on p. 164 has two objectives. Firstly, summarising some of the more well-known global corporate governance guidelines and regulations where risk management is included as either a recommendation or as a necessity. Secondly, providing a short overview of how risk management as part of corporate governance has developed from the 1990s in specific countries (CACG 1999:15; PWC 1999:44-48; IOD 2002:74-85; Spencer Pickett 2003:47-51; Corporate Governance Committee 2003; Basle Committee 2004; OECD 2004; FRC 2005; Lewis 2007; ASX Corporate Governance Council 2007:32-34; Marx 2008:106-172; ISO 2008; IOD 2009:72-80). Note that this is not a comprehensive

list, it merely aims to identify whether risk management is addressed in corporate governance guidelines.

Table 3.1: Inclusion of risk management in global corporate governance and other guidance

Country	Body	Date	Risk management
Global	Basle Report	1997 & 2004	Comprehensive risk management process for all financial institutions
	CACG	1999	Board must identify and manage key risks (principle 14)
	IFAC	2004	Risk management is the cornerstone of enterprise governance
	IIA	1999	Risk management is included in the revised definition of internal auditing
		2004	Position paper on the role of internal auditing in risk management
	IRM	2002	Comprehensive risk management standards
	ISO	2007	International standards on risk management
	OECD	1999	Board must ensure system for monitoring risks
		2004	Disclosure on risk factors Board responsible for risk policy
UK	Cadbury Report	1992	Encourage disclosure of specific key risks Risk management is based on the decision of the board
	Institute of Chartered Accountants (England & Wales)	1998	Proposed statement on risk management included in annual reports of publicly listed companies
	Turnbull Report	1999	Review of effectiveness of internal control system including risk management
	Smith Report	2003	Comprehensive guidance on implementing a risk management system
	FRC	2005	Emphasising the importance of risk management as part of an effective system of control
	Combined Code	2006	Board responsible for financial risk management system
Canada	Criteria of Control (CoCo)	1995	Risks must guide implementation of controls

Country	Body	Date	Risk management
	Board		
	Dey Report	2001	Board involved in function of risk management
USA	COSO	1992	Controls linked to objectives and risks threatening the achievement thereof
		2004	Comprehensive guideline for risk management ERM framework for all NYSE-listed companies
	NYSE	2003	Audit committee must discuss risk management process with management
Netherlands	Tabaksblat	2003	Management and board are responsible to implement and report annually
Australia	ASX	1995	All listed companies to include risk management in annual report
	Standards Board	1995 & 2004	Comprehensive standard on risk management
	Revised Code	2007	Detailed guidelines on risk management
SA	King Code	2002	Guidelines on risk management according to COSO report
		2009	Comprehensive guidelines on risk management

(Source: refer to discussion)

It seems that risk management is a later addition to corporate governance than the incorporation of internal auditing (compare table 2.4 on p. 91 and table 3.1 above), for example, risk management was not addressed in the first King Report (IOD 1994) whereas internal auditing, although with limited coverage, was included. However, it seems that some of the latest corporate governance codes and other guidance do not give internal auditing the same level of scope as that for risk management, for example, the UK's Combined Code, adding risk management as a new but dynamic dimension to corporate governance principles.

3.3.4.2 South African guidelines and legislation

As discussed in section 2.5.2.3 on p. 96 on the evolution of corporate governance guidelines in SA, the corporate governance process has not lagged behind global practices. This is also the case for the development of corporate governance guidelines with regard to risk management. In the first King Report (IOD 1994),

no mentioned was made of risk management. In table 3.2 on p. 166, the two remaining King reports (IOD 2002, 2009) are scrutinised to determine the growth in importance of risk management within SA organisations.

Table 3.2: Evolution of risk management in South African corporate governance codes

Topic	King II	King III
Board	• Total process of risk management • Set risk strategy • Understand risk aspects • Benchmark performance indicators • Determine risk appetite • Ensure annual risk assessment • Opinion on effectiveness of risk management systems • Disclosure in annual report • Management of significant risks	• Total system and process of risk management (comprehensive): ○ board charter ○ training of members ○ disclose in public statement • Risk management policy and plan: ○ adopt after design by management ○ annual review ○ support organisation's strategy ○ include: ▪ structure ▪ framework (approach) ▪ standards and methodology ▪ guidelines ▪ integration ▪ assurance • Determine risk tolerance (ability): ○ annually or at times of uncertainty ○ link with risk appetite (desire) ○ board limits linked to departmental, functional, activity and operational ○ monitor management's decisions • Monitor management
Manage-ment	• Design, implement and monitor risk and control systems • Commitment to process • Report to board	• Executive risk management plan and policy on daily basis • CEO accountable to board for design, implementation and monitoring systems and processes (resources and support provided by board) • Methodology and techniques embedded in strategy setting, planning and

Topic	King II	King III
		processes • Continuous monitoring and measure: o performance against indicators o progress against plan (deviations) o change in internal and external environment and impact on risks o effective and efficient risk response o trends, successes and failures o emerging risks
Risk committee (or audit com-mittee)	• Executive directors and senior management members • Duties: o consider risk strategies o monitor risk management on operational level o report to audit committee	• Executive, non-executive directors and senior management and independent experts (attend) • Minimum three members • Meet twice per year • Duties: o review risk maturity o effectiveness of overall risk management policy and plan o key risks addressed (review risk register)
Chief Risk Officer	• May appoint to assist	• May appoint to assist • Suitable experienced • Access to board and risk committee
Audit committee	• Determine assurance needed • Duties of risk committee if none	• Could use when no risk committee • At minimum have understanding of risk management process • Satisfy that following areas are addressed: o financial reporting risks o internal financial controls o financial reporting fraud risks o financial reporting IT risks
Internal audit	• Assist in monitoring (assurance)	• Independent assurance on integrity and robustness • Annual written assessment of effectiveness to board
Applica-bility	• Throughout organisation • Embedded in day-to-day activities	• Conceptual view directed towards objectives – long-term sustainability

Topic	King II	King III
		• Throughout organisation (strategic and operational levels) • Part of day-to-day activities
Commu-nication	• Risk policies to employees • Disclosure in annual report • Whistle blowing process for risks	• Stakeholders: o undue, unexpected and unusual risk o current, imminent or envisaged risks o effectiveness of risk management • Communicate policy and plan throughout organisation
Process	• According to first COSO Report model • Risk assessment determine controls implemented • Risk identification • Risk mitigation • Costs of losses • Risk register	• Risk assessment on ongoing basis (annually): o comprehensive, thorough, accurate and complete o methodology increases the probability of anticipating unpredictable risks o risk identification includes risks and opportunities o measure impact and likelihood o prioritise and rank risks o appropriate response
Types of risks	• IT • Assurance efforts	• All risks (comprehensive): o systematic o unpredictable

From the above, it is clear that the second King Report (IOD 2002) included a comprehensive discussion on risk management. However the third King Report (IOD 2009) has a much wider coverage of this topic. This added guidance can be interpreted as being either a positive or a negative contribution to the organisation and is discussed hereafter.

On the positive side, from the third King Report, it clear that the board of directors must take full responsibility for the total formal risk management strategy and it should form part of the organisation's strategic and business processes (Deloitte 2009; PWC 2009; Van Wyk 2009:10). Their guidance and leading by example ('tone at the top') will be the decisive factor as to whether or not management,

specific individuals and departments responsible for risk management, as well as all other employees, will take risk management serious. Another positive change is the more specific guidance to various role players, supporting the holistic approach (refer to section 3.7.1.2 on p. 217) including (Deloitte 2009; Ernst & Young 2009(c):6; Van Wyk 2009:10-11):

- the board having total responsibility;
- management being responsible for design and implementation activities, especially the risk management process;
- the risk committee assisting the board;
- the chief risk officer involved with the day-to-day responsibilities of risk management;
- the audit committee ensuring balance between risk management and other processes within the organisation; and
- internal auditing providing comprehensive assurance on the risk management framework.

With regard to specific aspects linked to risk management, the fact that comprehensive communication to related parties (for example, management to the board), other internal stakeholders (all employees), as well as all external stakeholders is expected, is a positive contribution to the third report. Without proper communication policies and structures in place, the objective of having a sound risk management framework will not be reached. People need to know what the risk culture of the organisation entails, what is expected from them and how they must contribute, as well as the outcome (positive and negative) of various risk management–related processes and systems. Lastly, both systematic (risks that are more predictable) as well as unpredictable risks are included in the report (Ernst & Young 2009(c):6).

On the negative side, some (Du Preez 2009; Newsome 2009) regard this section of the report as too comprehensive, making it more a list of rules instead of guidelines on principles. A further concern is that this section is very difficult to read with:

- certain topics being included in more than one area (for example, the duties and responsibilities of the board);
- topics not addressed under this section but another section (for example, audit committee);
- there is no logical flow (for example, from strategic level to operational level); and
- the terminology used is not consistent (for example, risk management procedures, structures, framework, plan or process); etc.

3.3.4.2.1 Private sector

In addition to the guidelines in the King reports (refer to section 2.5.2.3.1 on p. 101 for the implementation of these reports in the private sector), and the portions of the King reports' principles that are built into applicable legislation, other corporate governance guidance and regulations have been developed in SA on risk management for the private sector. These include, *inter alia*, the following:

- **Companies Act**

According to Section 94(7) of the Companies Act (SA – No 71 of 2008), the duties of the audit committee include performing any other tasks as stipulated by the board of directors, including an approach to evaluate and improve the effectiveness of the risk management process. Although the Act does not enforce risk management, it leaves the decision to implement a risk management framework in the hands of the audit committee.

- **Bank Act**

As mentioned in section 2.5.2.3.1 on p. 101, financial institutions globally have been affected by the current financial meltdown (refer to section 2.6.5 on p. 123) and are therefore included in the discussion. Section 60(A)(1) of the Bank Act, No 94 of 1990 as amended in 2003 (SA – Banks Amendment Act, No 19 of 2003) stipulates that banks should have a risk management framework. Section 64(A)

stipulates that a risk committee should be established and that the committee should ensure that an independent risk management function is established. Whether banks that went bankrupt, such as Lehman Brothers (Ellis 2008) in the USA, Northern Rock (Walayat 2009) in the UK and even Saambou Bank in 2002 (Bridge & Morris 2005) in SA, had adhered to such stipulations and regulations with a sense of responsibility, or whether they merely implemented these requirements (refer to section 2.6.2 on p. 117), is debatable.

3.3.4.2.2 Public sector

Apart from the King reports (IOD 1994, 2002, 2009) being applicable to the public sector, the SA government has addressed risk management within a legal framework in the PFMA (SA – No 1 of 1999) and Treasury Regulations (SA – National Treasury 2005) for national government, provincial government and public entities, within the MFMA (SA – No 56 of 2003) for local government, and provided further guidelines in the form of a risk management framework for the public sector (SA – National Treasury 2009) as well as for public entities within the Protocol on Corporate Governance (SA – Department of Public Entities 2002).

The former chairperson of the Public Service Commission, Professor Sangweni, declared that risk management is a key management tool for government in supporting accountability to the general public (SA – Public Service Commission 2003:i). This statement, as well as the PFMA, Treasury Regulations and MFMA legally enforcing risk management on the SA government, paved the way for the development of an integrated risk management framework for provincial government (SA – Public Service Commission 2002), best practices on risk management frameworks (SA – Public Service Commission 2003), and the National Treasurer's risk management framework for national and provincial government organisations (SA – 2009(a)). These are comprehensive documents (refer to table 3.4 on p. 193 for a discussion of the latter two documents) covering various concepts, tools and techniques to be used by management in the public sector when addressing risk management and are based on the COSO framework (COSO 2004).

- **Public Finance and Management Act and Treasury Regulations**

According to Section 38(1)(a)(i) of the PFMA (SA – No 1 of 1999), the accounting officer of public sector organisations must ensure that an effective and efficient risk management framework is implemented and maintained. The Treasury Regulations (SA – National Treasury 2005:3.2.1) built on the above and stipulate that the accounting officer must ensure that a risk assessment is conducted regularly to identify the emerging risks for the institution. It further addresses the need for a risk management strategy with specific requirements, including:

  - the compulsory inclusion of a fraud prevention plan;
  - the direction of the internal audit function's efforts and priorities;
  - the determination of managers' and staff's skills needed to improve controls and to manage these risks;
  - communication via a clear strategy to all officials; and
  - the incorporation of the risk management strategy into the language and culture of the organisation.

- **Public Sector Risk Management Framework**

This document, published by the Department of National Treasury (2009(a)), is a principles-based framework that is applicable to all spheres of government. It provides a comprehensive background on risk management within the public sector with specific reference to the oversight framework; drivers referring to a legal framework and governance guidance; enablers, implementers and supporters of the implementation of risk management; the process framework; tools and technology; and the assurance providers with comprehensive guidelines for internal auditing. Refer to table 3.4 on p. 193 for a more detailed breakdown of the framework.

- **The Protocol on Corporate Governance for the Public Sector**

This document (SA – Department of Public Enterprises 2002:31) is specifically for public-held organisations (also referred to as public entities) and extends the

stipulations of the PFMA and the Treasury Regulations. With regard to risk management it prescribes communication on various levels and to different parties on the progress as well as the outcome of the risk management framework. For example, the board should include a statement in all progress reports on the appropriate risk management policies and practices in place, as well as adequate systems to ensure compliance with these. The protocol also includes the fact that government, being a shareholder in any public entity, should be sensitive to commercial risks and thus needs detailed reports on these risks to be able to decide whether to choose to set limits on the exposure of government in certain situations.

- **Municipal Finance Management Act**

According to Section 62(1)(c) of the MFMA (SA – No 56 of 2003), the accounting officer must ensure that an effective, efficient and transparent system of risk management is implemented and maintained. Furthermore, Section 165 incorporates risk management into the assurance and reporting duties of the internal audit function, and Section 166, into the oversee duties of the audit committee.

3.3.5 Risk management standards

Many other guidelines have been developed to assist organisations in developing and implementing an effective and efficient risk management framework. In this section some of the most important and well-known guidelines and standards are briefly discussed. The actual model for a risk management process, if applicable to a specific guideline, is scrutinised in table 3.4 on p. 193.

3.3.5.1 Private sector

Various bodies have developed risk management standards to assist their members in the implementation of risk management. These standards attempt to provide a uniform set of terminology, risk management processes, and an

organisational structure or risk management framework. The following is a brief discussion of some of the most well-known standards available.

- **Institute of Risk Management (IRM 2002) – UK**

This document was developed collectively by the Institute of Risk Management, the Association of Insurance and Risk management and the National Forum for Risk Management (IRM 2002:1). Risk is defined, the risk management process is explained (refer to table 3.4 on p. 193) with appropriate tools and techniques, and the risk management framework, including the roles and responsibilities of various parties, is explained.

- **The Australian/New Zealand Standards Board (AS/NZS 4360:2004)**

These two countries jointly prepared a set of standards in 1999 and a revised set in 2004 on a generic framework for establishing risk management within an organisation. Apart from defining certain terminologies and describing the risk management process (refer to table 3.4 on p. 193), the standard also includes a discussion on how to develop, establish and sustain an effective risk management strategy according to the needs of the organisation.

- **COSO Report: Enterprise Risk Management (2004) – Global**

This is one of a few documents that have been developed for a global audience with the former IIA (SA) chairperson, Anton van Wyk, also contributing to the final product. Although the report contains discussions on terminology, the roles and responsibilities of various role players, limitations, and a few other crucial elements, its main contribution to risk management standards is its comprehensive guidance on the elements of the risk management process (refer to table 3.4 on p. 193). It includes a discussion on the internal environment of an organisation that will form the basis for all other components of the risk management process, consisting of the risk management philosophy, risk

appetite, commitment to competence, the organisational structure, the assigning of authority and responsibility, to name but a few.

- **International Organisation for Standardisation (ISO 2007) - Global**

ISO is a worldwide federation of national standards bodies that develops international standards for its members. ISO 31000 has been developed for guidance on risk management and includes a framework as well as a process (refer to table 3.4 on p. 193). With regard to guidelines on implementing a framework, the mandate and commitment of various parties are highlighted, including a risk management policy, integration of all processes into organisational processes, and accountability.

3.3.5.2 Public sector

As with the private sector, the public sector needs a plan or framework to address the risks with regard to service delivery faced by government organisations. Some of the most well-known guidance is briefly discussed.

- **Canadian Government (2001)**

The Canadian government (Canada – Treasury Board of Canada Secretariat 2001) has developed an integrated risk management framework (refer to table 3.4 on p. 193) that entails a one-page document approach where various types of strategic risks (including policy, operational, human resources, financial, etc.) for a specific organisation can be discussed, compared and evaluated. Although the use of the document is not compulsory, the President of the Treasury Board has urged public service employees to make use of the framework as it will most probably lead to a more holistic approach to risk management within an organisation.

- **United Kingdom Government (2002)**

The UK government (UK – Cabinet Office 2002(a):25-26, 2002(b)) developed a systematic approach with specific elements when addressing risks. According to this model (refer to table 3.4 on p. 193), the first step for a government organisation is to clearly stipulate the strategic objectives, explicitly to identify the roles and responsibilities of various parties, identify the objectives (aims) to be achieved, and the principles needed to guide action. The second step is to ensure that risk management is incorporated into the day-to-day activities of the government organisation. These include all employees being risk conscious when making decisions, implementing systems and processes to manage risks, and developing people skills for employees to be able to manage risks. The third step is to communicate the approach to all role players, and, lastly, management must not only drive the risk management process, but also the implementations of recommendations and improvements.

- **South African Government – Provincial (2002), National (2003) and National Treasury (2009)**

The first document, *Integrated Risk Management in the Public Service: a Provincial perspective* was developed by the Public Service Commission (SA – 2002) a body entrusted by the SA Constitution (No 108 of 1996) with the task of monitoring and promoting high standards of professional ethics in the public service. This document, although it briefly mentions the risk management framework, focuses on the progress of implementing risk management within the various provinces and, therefore, it will not be further included in this discussion on risk management guidance and processes.

The second document was also developed by the Public Service Commission (SA – 2003) to complement the PFMA (SA – No 1 of 1999) as the Commission was of the opinion that risk within the public sector has not received adequate attention in the past. The risk management process (refer to table 3.4 on p. 193) is complemented by a brief discussion on numerous risk management techniques

and models, as well as tools, templates and other relevant documents, including a risk register (refer to section 3.5.3 on p. 203). A further strength of the guidance is that it provides a risk management plan, including timetables, budgets and contingency funding, as well as best practices for risk management frameworks.

The third document was developed by the National Treasury (2009(a)) to assist all public sector organisations (national departments, provincial departments, constitutional institutions, public entities, provincial public entities, municipalities as well as municipal entities) to incorporate risk management not only into their strategic plan, but also their daily activities (refer to table 3.4 on p. 193).

3.3.6 Responsibilities of various parties

A risk management framework can only be successfully implemented if all the parties involved execute their responsibilities to the best of their ability. As debated before (refer to section 3.2 on p. 138), each organisation will have a unique corporate governance structure suited to addressing their specific needs. This is also true for a risk management framework. Therefore, the various parties involved as well as their tasks will differ from organisation to organisation. In this section the most common parties linked to the risk management framework and their roles and responsibilities are briefly mentioned.

3.3.6.1 Board of directors and risk committee

The board of directors is ultimately responsible for sound corporate governance structures including a risk management framework (COSO 2004:83; AS/NZS 2004:27; Spencer Pickett 2005:8-9; Atkinson 2008:42-45; IOD 2009:73-74). Their duties include, *inter alia*:

- setting the risk philosophy for the organisation as a whole;
- approving the risk appetite and risk tolerance that the organisation is willing to accept;
- understanding all the high priority risks;

- ensuring that the treatment of high priority risks is effective;
- ensuring that the overall risk management framework is efficiently implemented and maintained; and
- proper communication of risk management to all stakeholders.

The board mostly delegates these responsibilities to a board committee, being either the audit committee or, if appropriate or necessary, a separate risk committee. The risk committee's ultimate responsibilities are to ensure that the risk management framework is implemented and maintained, and to provide the board with assurance that the above is functioning as approved by the board. It also has the objective to ensure that the organisation's risk management framework keeps track of current best practices. Therefore it is advisable to have at least one risk management expert on the committee or, if needed, role players could be sub-contracted to assist in the detailed activities necessary to fulfil these tasks (Atkinson 2008:45; IOD 2009:75).

According to global studies (PWC 2006:34-36; PRMIA 2008; IIA Research Foundation 2009(b):50) on the status of global best practices of risk management, respondents indicated that their organisations either do have a risk committee (about one third) or are planning to implement one in the near future (approximately another third). Respondents also agreed that risk management should be a board priority. These statistics are even more favourable in SA organisations with 63% of the top forty companies listed on the stock exchange having a board risk committee (iKUTU 2009:45-56) and 90% of these respondents perceiving this committee to be an integral part of the organisation's risk management framework.

But is the board recognising and accepting its responsibility when it comes to risk management? According to a study amongst investors, executive management and board members (Ernst & Young 2009(a)), all those participating agreed that the board and the chief executive officer should take ownership of risk (Ernst & Young 2009(a):8) and that this is one of the most important contributing factors ensuring a successful risk management strategy. It seems that organisations'

boards are accepting this challenge. In a Deloitte study (cited in Beasley *et al.* 2008:44), the percentage of financial institutions acknowledging that oversight responsibility lies with the board rose from 57% in 2002 to 70% in 2008. However, the IIA Research Foundation (2009(b):12) found that only 39% of executive management and 52% of board members are of the opinion that sufficient information on risk reaches the appropriate decision making parties, with 51% of the respondents being satisfied with accuracy, 31% with completeness and 50% with the timeliness of information used in risk management activities. This raises the question as to whether the board can really take full ownership of risks if they are not properly informed. Is it the responsibility of the board to make sure they get the complete picture, or is it senior management's responsibility to provide them with it, or do both parties have a responsibility? Internal auditing is most probably in the best position to ensure that the board gets an overview of the whole risk management framework that is implemented and managed by the senior management team (refer to section 4.3.1 on p. 234).

3.3.6.2 Senior management and chief risk officer/risk department

The chief executive officer has as a main responsibility the establishment and implementation of the overall risk management framework, including a risk management process – thus the day-to-day activities that are in line with the board's vision. Thereafter, he/she has to align the strategic objectives with the risk appetite, as determined by the board, by managing the organisation's risk profile in compliance with its risk framework (SA – PFMA 1999:S38(1)(a)(i); COSO 2004:84-87; IOD 2009:75-76). These tasks are mostly delegated to a chief risk officer and/or risk department (De la Rosa 2007; Hettinger 2009:49). A chief risk officer must be positioned in the organisation where he/she has the authority to perform all the necessary tasks needed to ensure an effective and efficient risk management strategy. If needed, the chief risk officer may appoint further personnel to assist with these tasks, thus the establishment of a risk management department. The activities of the above role players include, *inter alia*:

- establishing and communicating the risk management department's vision;
- ensuring that other relevant parties, such as the risk committee, are properly trained on risk management;
- managing the risk function in terms of:
    - determining and implementing appropriate risk management infrastructures, policies and processes;
    - establishing methodologies and facilitating the use of tools and techniques;
    - facilitating risk identification and assessment;
    - implementing risk reporting structures; and
    - ensuring that risks are appropriately treated and monitored.

Summarising the view of prominent chief executives across the globe (Anonymous 2009:54-60), the future of risk management is a certainty with chief risk officers playing a more prominent role in a holistic approach, and the presence of a chief risk officer being positively associated with the scope of implementation of a risk management framework (Beasley *et al.* 2005:529). Global studies indicate that from approximately 80% of respondents' organisations (PWC 2006:36; PRMIA 2008:13) that do have a chief risk officer, to about 40% (Beasley *et al.* 2005:528; IIA Research Foundation 2009(b):35), most report to the chief financial officer or chief executive officer. It is, however, indicated by 82% (PRMIA 2008:13) of respondents that the chief risk officer should preferable report to the board. A company in the USA recently announced that they are adding the chief risk officer to the board of directors and investors responded by increasing the stock price by 7% (Lam 2009:24).

Concerning facts include that apart from the chief risk officer, 70% of organisations (PWC 2006:36) do not have other full-time risk management staff; the risk department's staff complement ranges from between one to three employees (IIA Research Foundation 2009(b):8); and the current credit crunch affecting many global banks has resulted in a poor job market for risk professionals (Campbell 2009:12). The status of the risk management division and/or chief risk officer is, however, complimented by the fact that many (between

30% and 40%) are actuaries, qualified risk managers or have a degree in a related field (Kleffner *et al.* 2003:59; PRMIA 2008:12). SA organisations mostly do have separate risk management functions with chief executives rating these departments' contribution to the risk assessment, risk management and risk communication processes as being significant (iKUTU 2009:46).

One of the areas that are highlighted in most of the studies on risk management, is the effective and transparent systems in place to communicate risk aspects (PWC 2006:10-11; Ernst & Young 2006:8-15; IIA Research Foundation 2009(b):4,11-13,17-18). This is primarily the responsibility of senior management that needs to provide information to the board, which in its turn needs to communicate with external parties. Studies indicate that organisations are primarily communicating through the annual financial statements, whereas investors want a more detailed briefing, such as the investors' presentation forum (refer to sections 3.2.3.2 on p. 147 and 3.2.4 on p. 150). To be able to report more comprehensively on risk management, the board and senior management will have to ensure that the information communicated is reliable. The internal auditors can play a vital role in providing this assurance (refer to section 4.3 on p. 232).

3.3.6.3 Internal auditing

In providing assurance on the implementation and maintenance of the above activities, internal auditing is in the best position to assist the board and senior management (COSO 2004:88; IOD 2009:80). The role of internal auditing in the risk management process is discussed in detail in Chapter 4.

3.3.7 Conclusion

Risk management is a new but dynamic addition to corporate governance with many benefits for the board as well as senior management. It is a structured framework that consists of numerous systems, processes and structures, involving parties across the organisation, to holistically manage risks. Corporate governance guidelines mostly include the concept of risk management, and are

complimented by other detailed guidance and standards on the topic. Most of these discuss the roles and responsibilities of certain parties, highlighting that without their commitment, risk management will not be able to reach its fullest potential.

3.4 THE CONCEPT OF RISK AS REFLECTED IN RISK MANAGEMENT

The general concept of risk is an everyday phenomenon, also occurring in the business environment and related professional disciplines. It thus has a variety of meanings and connotations such as threat or benefit, loss or opportunity, uncertainty or chance, probability of an event, or to dare, to name but a few (Bernstein 1996:1-8). In this section, risk as a generic term will be considered before investigating risk in the context of the business environment as well as risk management. Thereafter, risk as part of the business environment (business risk) will be scrutinised to identify the elements relevant to the corporate governance risk management framework, as well as the classification of risks to measure them within the context of a risk management framework.

3.4.1 Generic definition of risk

The word risk derives from the word *risicare,* which means 'to dare' (Bernstein 1996:8). According to dictionaries (Oxford Dictionary 2005:1009; Wikipedia n.d.(b)), in short risk is the possibility that a loss or harmful event that will cause a negative effect can occur. There are many other works that elaborate on this definition of risk and a few of the most important ones are analysed to identify common factors:

> The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood (IIA 2009(a):41).

> …uncertainty or loss, where both the degree of the uncertainty and/or the loss was not measurable. …deviation from the expected value. It implies the presence of uncertainty. There may be uncertainty as to the

occurrence of an event producing a loss, and uncertainty as regard to the outcome of the event. The degree of risk is interpreted with reference to the degree of variability and not with reference to the probability that it will display a particular outcome (Valsamakis *et al.* 2005:26-29).

…the chance of something happening that will have an impact on objectives…specified in terms of an event or circumstances and the consequences that may flow from it…measured in combination of the consequences of an event and their likelihood…positive or negative impact (AS/NZS 2004:4).

A hazard is the loss because of a certain occurrence. Risk, on the other hand, is two-dimensional including both the likelihood of the occurrence and its impact (loss). The level of risk is obtained by multiplying the two… (SA – Public Service Commission 2003:7).

…combination of the probability of an event and its consequences (IRM 2002:2).

Risk is the uncertainty of outcome, whether positive opportunity or negative threat of actions and events. It is the combination of the likelihood and impact, including perceived importance (UK – Cabinet Office 2002(b):10).

Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organisation's objectives (Canada – Treasury Board of Canada Secretariat 2001).

Absolute risk is a term for the threats and consequences without considering the controls likely to be present and operating (McNamee 1998 as cited in Prinsloo 2008:215).

From the above definitions, risk can be summarised as follows (also supplemented by discussion in Prinsloo 2008:220-223):

- Risk is an event(s) that occurs.
- This event is either a given (certain) or an unknown (uncertain). This uncertainty can be measured in terms of:
    - the probability of occurrence (likelihood); and
    - the effect (either positive or negative) on the outcome (impact).
- It is mostly impossible to measure the exact result of the outcome of the risk (the consequences being either a loss or a gain).

The above is the discussion of risk as an every day phenomenon taking place in different connotations that can be linked to many daily circumstances, for example, when crossing the road (event), a truck may come along (uncertain), strike the pedestrian (likelihood), cause injury (impact) and this could result in death (loss). According to various studies (Canada – Treasury Board of Canada Secretariat 2001; Valsamakis *et al*. 2005:26; Merna & Al-Thani 2005:11), to really understand risk it should be placed within a specific context, for example, the pedestrian and road environment (as described above) or the business environment.

3.4.2 Risk in the business environment

Business risk elaborates on the generic term of risk for the business environment and includes all the elements as summarised in section 3.4.1 on p. 182 but in so far as these are applicable for a specific organisation, both for the private and the public sector. The general definition of risk, as per dictionaries, mentioned in the previous section still applies to business risk in that it reflects a loss or harmful event causing a negative effect where the organisation will not reach its objectives. Various works reflect on risk within the business environment. A few of the most prominent are listed here:

> …the taking of risk for reward (IOD 2009:74).

The possibility that an event, activity or action will impact the ability of an organisation to execute its tactical and strategic business plans and achieve its business objectives (Sumners 2008).

Business risk is the probability of loss inherent in a firm's operations and environment…that may impair its ability to provide returns on investment (Business Dictionary 2007/8).

Business risk is a risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or form the setting of inappropriate objectives and strategies (SAICA 2009/10:Glossary 4).

Events can have a positive impact, negative impact, or both. Events with a negative impact represent risks…. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives… (COSO 2004:2).

The possibility that an event will occur [and] adversely affect the achievement of objectives (COSO 2004:124).

Risk refers to either uncertainty within the operational environment or the possibility that a specific event or events may derail a plan or service delivery outputs negatively (SA – Public Service Commission 2002:10).

Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organisation's objectives (Canada – Treasury Board of Canada Secretariat 2001:1).

Apart from the elements identified when summarising generic risk (refer to section 3.4.1 on p. 182) the following can be added for business risk (also supplemented by the analyses in Merna & Al-Thani (2005:14-16) and Prinsloo (2008:216-226)):

- Risks must be taken to be able to take advantage of opportunities. Risk is thus either a loss as a result of a negative outcome (hazard) or a loss of a potential positive outcome (opportunity).
- The outcome of risk is linked to the impact of the event, which will most likely be reflected in the reaching of the organisation's objectives, both on the strategic and operational levels (consequences of risks). These consequences can either be single or plural, positive or negative, and qualitative or quantitative.
- The source of risk must be identified to be able to manage the risk most effectively and efficiently. Sources are either physical (environmental) or moral (human, either accidental or deliberate) in nature (Ciechanowicz as cited in Prinsloo 2008:223).
- The cause of risk (why?) is the reason that will bring about the event that could become a risk and is mostly directly linked to the source.

From the above analysis of various definitions of generic risk as well as business risk, the concept of business risk could thus be defined as follows:

Business risk (coming from a specific source that causes the risk) is a certain or uncertain event, being either a hazard (something negative might happen) or a loss of opportunity (something positive does not happen), that may occur (likelihood) and may have an uncertain outcome (consequence) that has an impact on the organisation, usually reflected in the reaching of objectives, both strategically and operationally.

As evident from the above, no organisation can survive without taking risks. It is also true that risks can cause an organisation to go bankrupt or incur severe losses. The balance lies in the fact that risks should be taken in consideration of

the organisation as a whole and within a framework of risk management, ensuring responsible risk taking.

3.4.3 Business risk as part of corporate governance's risk management

The definition of risk management is discussed in section 3.3.2 on p. 155. In short, it is a structured framework to assist the board and senior management in ensuring responsible business risk taking. Linking the definition of business risk (see above definition) to risk management, there are a few elements that have a direct influence on this study and should be discussed in greater depth, namely uncertainty, risk as hazard and risk as opportunity. These are explained by means of appropriate examples in table 3.3 below. The effect of these elements on risk-based internal auditing includes the fact that auditors in general prefer to work with certainties and not with uncertain elements (Mayhew, Scatzberg & Sevcik 2001:52). Secondly, literature (PWC 1999:13; Spencer Pickett 2003:131; COSO 2004:16; Ramamoorti, Watson & Zabel 2008:53) indicates that organisations, including the internal audit function, tend to focus on risk as a hazard and ignore the loss of opportunity as a potential risk factor.

Table 3.3: Three elements of risk within risk management

Element	Example	Consequences
Uncertainty	Must organisation invest in producing a new product X?	Organisation invests – what if product does not sell? Organisation does not invest – what if product could have been a success?
Hazardous loss	Organisation decides to invest in producing product X	Product X is a failure and organisation loses development costs, manufacturing costs and reputation
Loss of opportunity	Organisation decides not to invest in producing product X	Competitor invests in product X and it is a huge success

3.4.3.1 Uncertainty relating to business risk

Uncertainty is the inability to know in advance (Bernstein 1996:219; COSO 2004:124) whether something will happen or not (likelihood) as well as the effect of the event (impact) if it does occur (Valsamakis *et al.* 2005:30). Uncertainty is directly linked to risk. When management takes risk by either being active or being passive, they are uncertain as to what the outcome of the event will be – including the possibility of either a hazardous loss or a loss of opportunity.

According to Merna and Al-Thani (2005:13) and Valsamakis *et al.* (2005:30-31) uncertainty is influenced by a number of factors such as a lack of clarity when structuring the problem, inability to identify alternative solutions, the quality and quantity of information available, the environment within which the risks are taken, the time available, and the repercussions of the influencing factors. Most of these factors can, however, be managed in a well-established risk management framework. Value is created when management takes informative decisions and balances growth and return with related risks. It is common knowledge that the board, as well as investors, does not appreciate uncertainty and surprises, especially those that affect the organisation in a negative way. With studies highlighting the importance of communicating risk-related aspects (refer to section 3.5.2.5 on p. 202), it is of great importance that risk as an uncertainty must be managed and communicated to all parties.

3.4.3.2 Loss as a result of threats (hazards)

Risks as a hazard embody the possibility that an action has a potentially negative outcome or consequence, including financial loss, fraud, theft, damage to reputation, injury, system failure or a lawsuit, to name but a few (PWC 1999:14; IRM 2002:7; Spencer Pickett 2003:131; COSO 2004:16; Merna & Al-Thani 2005:3-4). This is the more traditional way of focusing on risks and the management of these types of risks includes a more defensive attitude in preventing the events from happening. The cause of these risks could derive from seemingly positive conditions, which because they are not properly managed could result in a negative outcome. Thus, not all hazards have a negative origin.

For example, the demand for a specific product has increased (positive) and the organisation is lowering its standards to meet this demand. The lower standard products are sold and customers lose their trust in the products and the organisation, resulting in lower sales (negative).

3.4.3.3 Loss of opportunities

Risks embody the possibility that an opportunity to achieve something positive could be lost. This concept is based on the relationship between taking risks on the one hand, and return on the other – the greater the risk taking, the greater the potential return may be, but evidently, also the potential loss (PWC 1999:13; IRM 2002:7; Spencer Pickett 2003:132; Merna & Al-Thani 2005:3-4; IOD 2009:74). This type of focus on risk-taking is investment-driven, by either investing the organisation's resources in expanding business processes, or in pure investment transactions. The purpose is to take action in order to gain in the process. This could result in a loss, but, without taking the risk, a loss of opportunity could result in the organisation stagnating with no growth occurring. The answer lies in management knowing and understanding their organisation and the environment it operates in, and taking the risks that reflect in a positive way on the organisation. Thus, what will be an acceptable risk for one organisation may be the wrong choice or even devastating for another.

3.4.4 Types of risks related to risk management

Numerous types of risks exist (IRM 2002:3; Merna & Al-Thani 2005:17-25; Ernst & Young 2009(a); Richardson & Gerzon n.d.) that have an influence on organisations – either having an effect in the short, medium or long term, being externally or internally driven, or being strategic, operational, or financial risks. How different types of risks will influence organisations will depend on factors such as the type and size of organisation, the flexibility of operations, the environment in which it operates, and the risk-taking strategy of the board and management, to name but a few. However, a few categories of generic risks are applicable to most organisations, for example, holistic risks, static risks, dynamic risks, contingent risk, regulatory risks and reputation risks. Two of these types of

risk categories that are applicable to the risk management process are discussed in more depth, namely inherent risks and residual risks.

3.4.4.1 Inherent risk

Inherent risk is the possibility of an event occurring that could cause harm for an organisation in the absence of any preventative, corrective or detective measures (Spencer Pickett 2003:134; COSO 2004:122; SAICA 2009/10:Glossary-15; Prinsloo 2008:129-130; IIA 2009(e):par 4). The level of inherent risks will be directly related to the type of organisation and how it operates. The level of inherent risk is static and can only be changed when new strategies are taken. For example, an organisation that only operates (both purchasing and selling activities) within a single country will have no to minimum exposure with regard to import and export risks (low inherent risk). However, if an organisation has operations in various countries, import and export risks will play a prominent part in the risk management strategies, both on the strategic as well as operational levels (high inherent risk). The inherent risk-levels for these two organisations can only be altered by following a different strategy with regard to import and export operations. Therefore, although all organisations are exposed to inherent risks, the level of exposure of specific risks is directly linked to an organisation (Merna & Al-Thani 2005:19). Management needs to know the level of their inherent risks to be able to implement sufficient responses to mitigate the risks within a specific boundary or risk appetite (refer to section 3.5.2.3.1 on p. 200).

3.4.4.2 Residual risk

Residual risk refers to the remaining risks after management has taken action to mitigate the inherent risks by implementing appropriate responses (Spencer Pickett 2003:135; COSO 2004:124; IIA 2009(a):41; IIA 2009(e):par 4). The extent of the responses (for example, controls) that must be implemented to mitigate the risks is mainly influenced by the current inherent risk and the risk appetite of the board, that is the amount of risk that an organisation is willing to take. For example, where the inherent risk for global operations is high and the board has accepted a low risk appetite, numerous risk responses will have to be

implemented to lower the residual risk from high to low. Other factors that could influence the risk responses include the cost effectiveness compared to the benefits, risk tolerance (refer to section 3.5.2.3.2 on p. 200), the importance of the achievement of objectives, and the pursuit of new opportunities, to name but a few.

3.4.5 Conclusion

With the increased importance of risk management, the concept of risk as an uncertainty must be clarified before it can be managed. For the business environment, risk occurs when the organisation does not achieve its objectives, either as a result of a hazard, or a loss of opportunity. Risk can be managed by following a structured and systematic risk management process that lowers inherent as well as residual risk to acceptable levels.

3.5 RISK MANAGEMENT PROCESS

The definition of risk management is discussed in section 3.3.2 on p. 155 with reference to most of the prominent literature on the topic. However, there are some contradicting aspects relating to these definitions, with the most important being that some definitions refer to a process while others do not. Even within the King Report (IOD 2009) various terminology is used and this could be confusing to the reader (refer to section 3.3.2 on p. 155 for clarification of risk management framework and risk management process).

For the purpose of this discussion, both risk management and enterprise risk management (as discussed in section 3.3.2 on p. 155) are included when referring to a risk management process, whether, for a specific organisation, risk management is implemented in a silo or holistic approach. This section discusses the risk management process by first comparing the various models available, exploring certain of the elements of the process in more depth, and lastly explaining the function of a risk register.

3.5.1 Comparison of different models for a risk management process

Various models have been developed to assist with designing and implementing a risk management process. Table 3.4 on p. 193 summarises some of these models as per the task to identify common factors. Although there are numerous other models that have been developed by individual writers or researchers (refer to Prinsloo (2008:229) for a discussion of some of these), these will not be included as they reflect the view of either one or two individuals, or they have fewer elements per task than the models discussed.

With regard to the models that are compared, although the terminology may differ, all have certain uniting tasks that are further discussed. Where a specific document combines two or more tasks, it is addressed accordingly, for example, the document developed by IRM (2002) combines risk identification and assessment.

Table 3.4: Comparison of various risk management process models

Tasks	IRM (2002)	AS/NZS (2004)	COSO Report (2004)	ISO (2007)	Canadian Government (2001)	UK Government (2002(a) and (b))	SA – National Treasury (2003 & 2009(a))
1 Objective setting	• Strategic	• Context: ○ internal ○ external ○ criteria	• Objectives: ○ strategic ○ operational ○ reporting ○ compliance	• Context: ○ internal ○ external ○ criteria	• Identify issues • Set context	• Strategic • Programme • Project	• Context: ○ strategic ○ sector ○ operational • Scope
2 Risk identification	• Risk analysis: ○ identification (i.e. strategic, operational, financial & compliance) ○ description (i.e. scope & nature) ○ estimates (threat & opportunity's consequences & occurrence)	• What, where & when • Why and how • Tools & techniques	• Events (categories) • Influencing factors (cause) • Techniques • Hazards & opportunities	• Sources • Events • Consequences • Tools & techniques • Hazards & opportunities		• Empirical • Imaginative	• Circumstances • Consequences • Risk categories • Source
3 Risk assessment		• Analysis: ○ existing controls ○ consequences & likelihood ○ types: ▪ qualitative ▪ semi-	• Inherent and residual risks • Likelihood and impact • Techniques • Risk appetite and risk tolerance	• Tolerance • Meet criteria	• Analyse • Measure: ○ impact ○ likelihood • Rank	• Measure: ○ trends ○ quantify ○ evaluate • Judge: ○ values ○ ethics ○ public view	• Inherent and residual risks • Attributes: ○ impact ○ occurrence • Classification (low – high) • Evaluate

	○ techniques • Risk evaluation: ○ accept ○ treat	quantitative ▪ quantitative • Evaluate				○ Other issues, e.g. social, political, economy	• Risk rating
4 Response to risks	• Types: ○ control ○ avoid ○ transfer ○ finance • Cost effective	• Positive outcome: ○ start/continue ○ change impact /likelihood ○ share • Negative outcome: ○ avoid ○ change likelihood/ impact ○ share	• Types: ○ avoid ○ reduction ○ share ○ accept • Controls • Cost and benefits	• Treat: ○ avoid ○ change likelihood/impact ○ share ○ retain ○ continue • Select option • Implement	• Desired results • Options • Select strategy • Implement	• Policy: ○ options ○ cost ○ suitable • Assurance on controls	• Types: ○ avoid ○ reduce ○ transfer ○ insure ○ retention • Responsibility • Resources & budget • Timeframe
5 Communi-cation	• Internal • External	• Record process	• Information • Internal • External	• Record process	• Consultant • Wide range of activities	• Various levels	• Periodic/timely • Relevant • Improve
6 Monitoring	• Structure	• Ongoing • Learn lessons	• Ongoing • Separate & evaluate • Deficiencies	• Learn lessons • Regular check, e.g. audits	• Improving	• Contingency • Consequence management	• Accurate • Timely • Ongoing • Separate (audit)

(Source: refer to table headings)

3.5.2 Elements within the risk management process

Table 3.4 on p. 193 is a summary of prominent risk management processes that have been developed by various bodies worldwide as part of risk management standards (refer to section 3.3.5 on p. 173 for the relevant risk management standards). Seven common tasks are included in most of these documents (some tasks are combined in certain documents) and the documents used in table 3.4 are further investigated with regard to these.

3.5.2.1 Objective setting

In table 3.4 on p. 193, four models refer to strategic objectives, two refer to operational objectives and a third to programme and project objective setting that could also be interpreted as operational objective setting. Most organisations have a vision and mission statements that set out what the organisation wants to achieve. Based on the vision and the mission, the organisation establishes strategic objectives or high-level strategies that determine the path that needs to be followed to achieve the vision and the mission. Organisations also normally consist of numerous business units (for example, human resource department) and business processes (for example, payroll) that will be determined by the type of organisation and the way the organisation does business. Operational objectives are set to enhance the effectiveness and efficiency of activities and should be developed in alliance with strategic objectives. To successfully apply risk management, the entire scope of an organisation's activities must be monitored, including high-level activities (strategic planning), business unit activities, and business processes (operational planning).

In setting the strategy for the strategic objectives, management considers risks relative to alternative strategies as a specific strategy may have a higher return and lower risk or *vice versa*. Thereafter, operational risks are developed to compliment the strategy. Without operational risk management, a business unit or process could hamper the reaching of strategic objectives, which could in turn cause much damage for the organisation as a whole. Therefore, it is crucial to manage risks on both the strategic as well as operational level.

In studies performed amongst various role players in the risk management framework (PWC 2006:12; IIA Research Foundation 2009(b):28), the importance of managing risk on an organisation-wide basis (referring to the term enterprise risk management) is increasing. This includes both strategic as well as operational levels.

3.5.2.2 Identification of risk

The term risk identification refers to the process of identifying all the risks that may influence the reaching of the organisation's objectives. The documents discussed in table 3.4 on p. 193 use varying terminology, as explained below:

- Management identifies potential events (uncertainties, hazard and/or opportunities) that are affecting, or that could affect an organisation's ability to successfully implement strategy and achieve objectives.
- As a result of constant change in the internal and external environment of an organisation, management should continuously identify risks.
- Management will have to investigate and determine the applicable:
    - risk areas (risk categories, risk exposure areas or circumstances affecting the organisation);
    - individual risks (things that can go wrong within the risk area);
    - risk factors (the cause of the risk);
    - source of the risk; and
    - consequences or results of the risk.
- The identification of risks is a systematic and logical process (empirical), but also requires the insight and imagination of the participants.
- Various tools and techniques have been developed to assist management with this step.

Thus, a formal and structured risk identification process is needed to ensure that all the relevant risks for a specific objective are identified.

Prinsloo (2008:232-236) discusses various risk identification approaches:

- The statistical approach uses historical information in a frequency distribution chart that is used to identify potential future risks.
- Exposure analysis categorises the area under review according to its exposure, risks are then identified per category (also used by most of the models in table 3.4 on p. 193), for example, physical assets – plant and equipment.
- The environmental approach refers to the various environments and sub-environments that an organisation is exposed to, for example, the physical environment such as the location of the organisation, economic environment such as interest rates, or government regulation such as legislation.
- The risk scenario approach refers to the identification of risks as a result of hazards, for example, potential fraud or threats that only exist for a short period of time.
- Checklists with numerous 'what if' questions can be used to identify risks.
- Key indicators or influencing factors such as legal factors and market factors can also be used for risk identification.

Studies amongst parties responsible for the risk management process underline the importance of the risk identification step. One of the most prominent reasons for implementing risk management in the first place is to identify common risks so that they can be addressed efficiently (IIA Research Foundation 2009(b):29). This identification of common risks is then upgraded to a 'complete as possible' list of risks identified by using a more structured process. Lastly, the risks are categorised to ensure that all relevant exposure areas are addressed (PWC 2006:7-10; PRMIA 2008:13-16).

3.5.2.3 Assessment of risks identified

Once risks and other relevant factors have been identified, an assessment that includes the analysis, measurement and evaluation of each risk should be conducted. Table 3.4 on p. 193 uses various terms, many of which are actually the same concept. The next paragraph explains the meaning of each within the context of the risk management process.

Although numerous tools and techniques exist, the assessment should include both the possible impact (linking a value to the damage or loss of opportunity that is, or could be caused) and corresponding likelihood of occurrence (how often it occurs, or could occur). It is important to use consistent parameters that will make it possible to develop a prioritised risk map. For example, risks should be first assessed according to inherent risk (gross risks – refer to section 3.4.4.1 on p.190), and after taking existing controls and other procedures into consideration, according to residual risks (net risks – refer to section 3.4.4.2 on p. 190). Lastly, the measurement can either be qualitative (personal judgement) or quantitative (measured in terms of trends or other statistical information). For both these measurement techniques, specific values must be linked for all the levels. For example, when using low-, medium- and high-impact, low should be < R500 000, medium between R500 000 and R2 000 000, and high > R2 000 000.

The outcome of this step is a list of individual risks for the organisation, assessed in terms of:

- high, medium or low;
- qualitative or quantitative; and
- impact and likelihood.

According to Prinsloo (2008:238-239) three approaches exist to analyse, measure and evaluate the risks identified, namely:

- various statistical methods;

- the risk factor approach that integrates perceptions of risks, consequences and controls into observable events; and
- the matrix approach where the subjective views of management are used to set an average (most commonly in use – refer to figure 4.3 on p. 277 for an example).

A study performed by PWC (2006:42-43) on the implementation of a risk management process reveals that organisations consider the risk identification and risk assessment elements as being the most valuable in the process and thus these elements are usually the furthest developed. Numerous tools and techniques exist (Merna & Al-Thani 2005:55-88) that can be used with the above approaches. Interviews (66%) and guided judgement (60%) are identified in the study performed by the IIA Research Foundation (2009(b):46-47) as most commonly used. These methods are very subjective and could result in sacrificing the accuracy, completeness and timeliness of information used during the risk assessment process. A previous study performed by the IIA Research Foundation has highlighted risk workshops as a more effective but costly approach (Walker, Shenkir & Barton 2002:21-22).

It is not always possible or cost-effective to eliminate risk entirely and the assessment of risk gives management the opportunity to evaluate each risk and then decrease it to an acceptable level or within a specific target. Many events are recurring and routine in nature and could possibly already be addressed in management programmes. Others are unexpected, often having a low likelihood but may have a significant potential impact or *visa versa*. It is therefore important to determine both the impact and the likelihood of each identified risk, measure each risk against a predetermined boundary, and decide how to treat each risk. The boundaries are the risk appetite or tolerance of the organisation (refer to table 3.4 on p. 193) as explained in the next two sections.

3.5.2.3.1 Risk appetite

The concept of risk appetite refers to the amount of risk an organisation is willing to accept in pursuit of value, (COSO 2004:19) thus setting boundaries. This is usually a decision made by the board and can be qualitatively- (high, medium or low) or quantitatively- (specific numeric values) based. The risk appetite is directly linked to the risk response (refer to section 3.5.2.4 on p. 201) and is influenced by the risk culture of an organisation. This is the set of shared attitudes, values and practices that determines how an organisation considers risk in its day-to-day activities. Although the risk culture affects the implementation of risk management within the organisation, the risk culture is affected by the overall organisational culture (Kimbrough & Componation 2009:24).

3.5.2.3.2 Risk tolerance

The risk tolerance provides an acceptable variation or deviation from the risk appetite to ensure that objectives are achieved. For example, if the risk appetite based on benchmarking is three mistakes, the risk tolerance could increase this to four mistakes.

In most guidelines (refer to section 3.3.4 on p. 163) the board is the party responsible for setting the risk appetite. However, studies reveal that this set risk appetite is then not being communicated to all relevant parties, with 61% of chief audit executives, a prominent party within the risk management framework, not receiving such information (IIA Research Foundation 2009(b):43). Without the establishment and proper communication of the risk appetite, the risk management process cannot succeed. The mere identification of risks, although a very important step, is only the foundation of the rest of the process. Risk that is identified must be measured against predetermined criteria and managed according to the outcome. If no criteria or risk appetite are set, the risk management process is meaningless.

3.5.2.4 Risk responses

After assessing the organisation's risk profile, management needs to determine how to treat the risks, also referred to as risk responses. According to table 3.4 on p. 193, the following responses can be chosen:

- Avoid (five models) the risk by not taking the action that gives rise to risk, for example, deleting a product line or selling a division (usually high likelihood and impact).
- Reduce, treat or mitigate (six models) the likelihood or impact of the risk by implementing controls, and other risk mitigating procedures (usually low impact but high likelihood).
- Share or transfer (five models) the risk by transferring or sharing some of the risk with other parties, for example, insurance or outsourcing (usually low likelihood but high impact).
- Accept or tolerate (four models) the risk by taking no action to manage the risk, for example, if it is not cost effective to implement controls (usually low likelihood and impact).
- Exploit the risk if an opportunity is present (IOD 2009:78).
- Terminate the activity that gives rise to the intolerable risk (IOD 2009:78).
- Integrate some or all of the possible risk responses listed above (IOD 2009:78).

The boundaries as set by the board (risk appetite and risk tolerance) as well as the type of organisation and its risk culture will influence the decision as to which response to choose. Another factor that could play a role is the cost-effectiveness of the response. According to table 3.4 on p. 193, three of the models discuss the cost-effectiveness of the risk response in terms of which response to choose, and although risk responses sometimes have to be chosen without considering the cost-effectiveness, in many instances it will have an impact on management's decision. The study by PRMIA (2008:18-19) provides a holistic view on this aspect. It emphasis the fact that failing to implement a risk management process, including the appropriate risk response, on the grounds that it is too expensive, is

not an option. As risks are uncertainties, it could be more costly should surprises arise, such as the current financial crisis affecting the world, and risk responses should be implemented to create a competitive advantage.

3.5.2.5 Risk communication

According to table 3.4 on p. 193, communication with regard to the risk management process should be both internal and external (two models), and suitable information that is properly documented (four models) should be kept of the whole process.

Studies indicate that although personnel responsible for the risk management process have sufficient systems in place to communicate the outcome of the risk management process to all relevant parties (PWC 2006:10), much still has to be done by the board and senior management with regard to proper internal communication to enhance the importance of the process (IIA Research Foundation 2009(b):42-43).

3.5.2.6 Risk monitoring

With regard to monitoring, the most important aspect is that it should be an ongoing process (five models), incorporating lessons learned from past experiences (four models), and that it should be a structured process including a separate evaluation from another party (four models), such as internal auditing.

Although this step in the process seems to be the least important, the lack of proper monitoring will most probably ensure that the risk management process, over a period of time, becomes void. Without feedback in terms of the risk management performance, management will not know whether all the relevant risks that have been identified are addressed appropriately, as well as whether new emerging risks are identified and included in the risk management process (Lam 2009:26). Research amongst chief audit executives indicates that the implementation of continuous monitoring still needs to be fully understood by management with only 46% of respondents indicating that the review of risk

management efforts does occur, 24% indicated that risk management performance measures are in place and only 50.6% were moderately to highly satisfied with their ongoing risk management monitoring activities (IIA Research Foundation 2009(b):42,49).

3.5.3 Risk register

A risk register is one method of keeping track of all the information gathered during the risk management process. A risk register is a document that should be regularly updated as new risks, both on the strategic as well as operational level, are identified, assessed and responded to. It should at minimum include the following information (SA – Public Service Commission 2003:21-22; AS/NZS 2004; Merna & Al-Thani 2005:59-61; Griffiths 2006(a):23; De la Rosa 2008(b); Campbell 2008:55-57; Baker 2009):

- appropriate dates;
- objective(s);
- risk appetite/tolerance;
- risk category(ies) for each specific objective;
- risk(s) for each risk category;
- inherent risk (both impact and likelihood) for each risk;
- risk response(s) for each risk;
- residual risk (both impact and likelihood) for each risk;
- risk owner;
- management's action plan for risks above risk appetite/tolerance;
- implementation date or due date; and
- follow-up performed.

Apart from using the risk register to document all the information gathered during the risk management process, it can also be used in the internal communication structure to update line managers on risks within their departments and how these are managed, and to notify senior management and the board of new emerging risk exposures that need immediate attention. Additionally, it can be

used to effectively locate the owner of the risk and check how he/she is managing the risk. Although the board ultimately remains the owner of all risks, the day-to-day responsibilities of managing the risks are delegated to specific individuals. With a proper risk register, management will have a better idea of what is being done by whom, and risk owners will be kept on their toes to ensure that risks are kept within the risk boundaries. Lastly, the register can also be used by the internal audit function when performing a risk-based internal audit engagement approach (refer to section 4.5.3.2 on p. 266).

Only one study (Crawford & Stein 2004:506) has been identified where the existence of a risk register is investigated – 80% of the responding organisations had some form of a risk register. However, a worrisome fact is that organisations tend not to use technology to assist with the risk management process (IIA Research Foundation 2009(b):55) and that this has an impact on the effectiveness and efficiency of the process, as well as the level of satisfaction of related parties with regard to information received (IIA Research Foundation 2009(b):58). Considering the magnitude of information that is gathered when a full-scale strategic and operational risk management process is implemented, technology can be an effective and efficient aid to make sure that the information is reliable and managed in a timely manner (Baker 2009; IIA 2009(e):par. 11).

3.5.4 Conclusion

Good business principles require that a risk management process should be performed on an ongoing basis, especially when change takes place. In SA, guidance requires that it should be performed on a continual basis (King Report – IOD 2009:76) or on a regular basis (Treasury Regulations – National Treasury 2005:par. 3.2.1). The board of directors should take responsibility for the process, and if an organisation has a risk department and/or risk officer, the task is usually delegated to them. Most importantly, a proper process to document all activities and communicate to all parties is essential for the success of a risk management process.

3.6 RISK MATURITY

Within the context of this study, risk maturity plays a very significant role as only organisations that are risk mature are included in the empirical study (refer to section 1.8.4.2.1 on p.44) and risk maturity plays a vital part in how internal auditing can incorporate risk into their activities (refer to section 4.5.3.1 on p. 264). It is therefore appropriate to introduce the concept and interpret the meaning of risk maturity, as well as analyse different measurement models to provide a common list of measurement criteria used.

3.6.1 Introduction

Risk maturity provides role players with a way to combine all the various elements of a risk management framework to best suit the needs of their organisation. The more relevant activities and elements of the risk management framework management have implemented effectively, the more risk mature the organisation is. A risk maturity model provides a stepping-stone approach to assist organisations in progressively reaching the desired maturity levels. The benefits of using a maturity model when determining the risk maturity level are increasingly being recognised by individuals, organisations and governments worldwide (Lenckus 2006; McDonald 2007:28; Chapman 2009). The model is primarily used by risk managers to measure how advanced their risk management framework is and to communicate this information to senior management and the board, which, in turn, can incorporate this information into their decision making with regard to risk management strategies. Secondly, the assessment will provide role players with areas that need improvement within the organisation's risk management strategy, providing an action plan for the development of the risk management framework.

Various descriptions of the term risk maturity or the different stages of adoption of the risk management framework within an organisation exist, namely:

> …a risk maturity model is a generally accepted reference model or framework of mature practices for appraising an organisation's risk

management competency. Experience has shown that risk management maturity can be described as a series of distinct incremental steps which progressively derive greater benefits. A maturity model is a structured collection of elements that describe characteristics of effective processes (Chapman 2009).

The risk maturity model provides a standard by which organisations can evaluate and improve their approach to ERM [Enterprise Risk Management]. The risk maturity model features a real-time benchmarking exercise that allows executives to score key characteristics of their risk management programs and generate a personalised maturity assessment (Liebowitz 2007:44).

The extent to which a robust risk management approach has been adopted and applied, as planned, by management across the organisation to identify, assess, decide on responses to and report on opportunities and threats that affect the achievement of the organisation's objectives (De la Rosa 2008(b)).

When the risk management philosophy is well developed, understood and embraced by its personnel, the entity is positioned to effectively recognise and manage risk. Otherwise, there can be unacceptable uneven applications of enterprise risk management across business units, functions or departments (COSO 2004:28).

Risk maturity is thus:

- a series of steps;
- that evaluate and score key characteristics of the risk management framework;
- against best practices (benchmarking);
- to determine whether the risk management framework as adopted and planned by the board and senior management, has been adhered to.

A risk maturity model is:

- a structured and systematic approach;
- with a list of current generally accepted criteria;
- that is used as a benchmark against which to evaluate the organisation's risk management framework;
- to determine the maturity or level of implementation of the risk management framework.

It is important to use a well developed risk maturity model to ensure that the result of the comparison makes sense within the global risk management environment (macro level) and can be trusted by the organisation's risk managers as well as the board and senior management (micro level). In table 3.5 on p. 209 a few of the risk maturity models currently in use are compared.

Although it would seem to be a fair assumption that all organisations would want to strive for the highest risk maturity level, this is not always the case as the highest level is not always the best option. A high risk maturity level may have some disadvantages including that it may be very expensive and time consuming. It may not be necessary for a specific organisation to implement all the elements of a risk management framework to manage its risk effectively and efficiently to ensure that objectives are achieved. The risk maturity of the organisation has to be decided by the board, as overall custodians of the risk management framework. The board is, in turn, guided by risk managers and senior management.

3.6.2 Risk maturity model

In this section various models and best practices frameworks are compared with one another to determine common criteria that are used to measure risk maturity. Maturity models are much needed barometers for risk management role players. With risk management being a relatively new addition to the corporate governance environment, much guidance is needed to ensure that organisations'

mitigate their risks optimally – not over- or under-managing – but to reach objectives effectively and efficiently.

Most maturity models are based on the Capability Maturity Model that was developed by the Software Engineering Institute (SEI) in the USA in the 1980s (Liebowitz 2007:44; McDonald 2007:29; Chapman 2009). According to this model, maturity models should be in the form of a matrix that comprises the following elements:

- a few levels of maturity describing the stage of development;
- the assessment criteria or attributes describing the quality of the risk management practices within each level; and
- the competencies describing the incremental improvements or desired capabilities, linking the levels to the criteria.

A few of the most well known models are compared to determine which risk maturity models address all three of the above areas,.

3.6.2.1 Comparison of different models

Although the concepts of risk maturity and a risk maturity model are new to the business environment, a few risk maturity models were identified after undertaking a comprehensive search. It is possible that other risk maturity models do exist, but for the purpose of this study, where risk maturity is not the main objective, it was decided that these models were sufficient to address the benchmarking of risk maturity models. Table 3.5 on p. 209 compares some of these models by measuring them against the Capability Maturity Model's three elements (refer to section 3.6.2 on p. 207), namely maturity level (all adhere), the criteria used (only three models adhere), and the measurement criteria (all adhere).

With regard to the models used, the Massachusetts Institute of Technology, Center for Transportation and Logistics model (MIT n.d.) was developed for the mitigation and elimination of risks in supply networks. The Hillson model (1997), International Association for Contract and Commercial Management (IACCM) Business Risk Management Maturity model (2002), Hopkinson model (2004) and RIMS model (2006) were develop as generic tools for organisations to determine their risk maturity and then, guided by the outcome, to determine the further implementations needed to become more risk mature. The IIA (UK and Ireland) model (2003) and the Spencer Pickett model (2005) were developed to assist internal auditors in determining the level of the organisation's risk maturity in order for the internal audit function to decide what their role should be in the risk management framework – ranging from providing advice (risk immature) to providing assurance (risk mature).

Table 3.5: Risk maturity models

Model	**Maturity level**	**Criteria used and measured against capabilities**			
Hillson 1997		Culture	RM Process	Experience	Application
	Naïve	No awareness	No process	No understanding	No structured application
	Novice	Selected use	Some methods	Individuals	Inconsistent
	Normalised	Policy & benefits	Formal process	In-house training	Routine
	Natural	Top-down commitment	Comprehensive	All staff aware	All activities
IACCM 2002		Culture	RM Process	Experience	Application
	Novice	No awareness	Inefficient	None	Not used
	Competent	Some awareness	Inconsistent	Basic	Inconsistent
	Proficient	Understand benefits	Consistent & tailored	Proficient	Adequate resources
	Expert	Proactive & full commitment	Adaptive & fit for purpose	Extensive experience	Proactive resources
IIA (UK & Ireland)	Naïve Aware Defined	No formal approach Scattered silo-based approaches Strategy and policies in place and risk appetite defined			

Model	Maturity level	Criteria used and measured against capabilities						
2003	Managed Enabled	Organisation-wide approach Fully embedded in operations						
Hopkin-son 2004	 Naïve Novice Normalised Natural	Measured in terms of stakeholders, risk identification, risk analysis, risk mitigation, project management and culture: Little attention paid to actions Progress against planned implementation not satisfactory Process against planned implementation usually satisfactory Actions carried out in consistent professional manner						
Spencer Pickett 2005	Awareness Design Integration Review	Some form of system is needed to ensure a methodical approach to manage risk System(s) is designed for risk management process incorporation Systematically apply risk management throughout organisation Reporting structures to ensure processes are functioning optimally						
RIMS 2006		Approach	Process	Appetite	Cause	Uncover risks	Perform	Sustain-ability
	Ad Hoc	Little account-ability	Reactive	Silo view	No cost saving	Own by specialist	Limit measure	Aware
	Initial	Compliance enforced	Need recognised	Only senior level	No top-down	Lists of risks	Separate process	Broader view
	Repeatable	Understood	All needs	Communicated	Understood	Growing lists	Contributes	Far-sighted
	Managed	Self-governed	Define & enforce	In each step	Implement	Owners manage	Integration	Comprehensive
	Leadership	Strong	Embedded	Delegate to all	Mitigate	Best practices	Performance measure	Continuity
MIT Not dated	1 2 3 4	Able to respond to most disruptions Minimise disruptions and recover fast Planning and execution are integrated Strategic initiative integrated into operational management and external reporting						

(Source: refer to discussion)

When the risk maturity models are compared with the Capability Maturity Model developed by the SEI, only three of them have all three elements in their structure – the models developed by Hillson (1997), the IACCM Business Risk

Management working group (2002) and RIMS (2006). Furthermore, it is evident that the RIMS (2006) model is by far the most comprehensive tool when it comes to measuring risk maturity (refer to table 3.5 on p.209). Thus, in Annexure E on p. 466, a comprehensive list of all the criteria of this model is provided. Additional to the above, it also has a list of criteria (refer to Annexure C on p. 460) and a list of deliverables (refer to Annexure D on p. 463).

For the purpose of deciding which common criteria should be included in a comprehensive risk maturity model, only these three models will further be investigated.

3.6.2.2 Common criteria used

The Hillson model (1997) and IACCM model (2002) have four criteria whereas the RIMS model (2006) has seven criteria. These models' criteria are briefly discussed after being compared with one another to determine which criteria should be used when measuring an organisation's risk maturity levels. Additionally, when scrutinising the documents, it seemed as though some of the different criteria overlapped and addressed the same concepts, and as such, even though different terminology is used, these criteria can be meaningfully combined.

- **Criteria: culture, approach and appetite**

This describes the attitude, commitment and degree of support from the board and senior management with regard to risk management, referring to the extent to which the risk management framework is adopted and implemented. It includes aspects such as setting a risk management policy (including the determination of the risk appetite), the level of integration of various risk management initiatives across the organisation, starting with the integration of risk management within the strategy setting process, internal and external communication (including the overall awareness of the importance of risk management), and the coordination between various parties.

- **Criteria: process, cause and uncover**

This refers to the steps and initiatives undertaken to identify, assess, evaluate, mitigate and monitor risks. It includes the integration with other business processes as well as the risk appetite accepted by management, and how the accountability of various parties is used to guide decision-making and eliminate gaps. Previously it was concluded that the identification of risks is a very important step in the risk management process (refer to section 3.5.2.2 on p.196). Therefore, the RIMS model specifically refers to the gathering or uncovering (identifying) of risks using risk management tools, as well as the identification of the root cause of the risk, as this will guide the risk manager during the mitigation step.

- **Criteria: perform and application**

This criteria refers to the application as well as the performance measurement of the adequacy of the risk management framework, with reference to aspects such as resource allocation, policies, the risk management process, implementation of the risk response within the boundaries of the risk appetite, quality of communication, and the achievement of objectives, to name but a few.

- **Criteria: sustainability**

This could be difficult to measure, as sustainability, including resilience, is difficult to gauge. Linking these concepts to risk management further complicates the measurement. However, this criteria could be measured in terms of the integration of risk management within the operational activities of the organisation and, understanding the consequences of a risk, whether actions are taken to mitigate the risk, or whether it is accepted within the boundaries of the risk appetite, for example, supply chain disruption or a major change in the market pricing.

- **Criteria: experience**

Personnel should be equipped and supported to manage risk well. This includes that risk tasks should be performed by qualified staff with the appropriate range and depth of knowledge needed, skills, competencies and a positive attitude. Furthermore, management should ensure that sufficient resources are allocated to the staff, and training or personal development are provided.

3.6.3 Conclusion

The risk maturity of an organisation will have an enormous effect on the various criteria implemented with regard to the risk management framework. For this study, only organisations that are risk mature will be included in the empirical study as risk maturity is a prerequisite for risk-based internal auditing (this is debated in section 4.5.3.1 on p. 264). The following criteria according to the analysis of the various risk maturity models are used to determine risk maturity (refer to Annexure F for the risk maturity scorecard used in the empirical study):

- Risk management approach including:
  - culture;
  - involvement in strategy setting;
  - risk management policy setting (including the risk appetite); and
  - reporting and communication.
- Risk management process including:
  - cause; and
  - uncover.
- People or staff experience.
- Risk management application and performance measurement.
- Sustainability.

3.7 FUTURE OF RISK MANAGEMENT

Many well-known organisations such as the insurance giant AIG in the USA had risk management frameworks in place but still suffered losses as a result of the current global financial crisis (Killackey 2009:28; Lam 2009:22). This raises the question whether a formal risk management framework is indeed worthwhile when taking into consideration the cost and effort it takes to implement. This question could probably be answered by scrutinising the weaknesses and gaps within the implementation of an effective risk management framework. This section first discusses the factors playing a role in the failure of the implementation or application of risk management. Thereafter, current trends and new developments that could eliminate the problems are discussed.

3.7.1 Possible weaknesses in the implementation and application of risk management

Failures in the implementation of effective risk management can be classified into two groups – the organisation is either risk ignorant and, as such, it does not have a proper risk management framework in place, or the organisation is risk competent and does have a proper risk management framework, but does not make the right decisions as a result of the risk culture embedded in the organisation (Lam 2009:23). The banking industry was seen as the leader in risk management (Baker 2008:34), but the global financial crisis, that affected this sector the most, was a direct result of poor risk management principles (Financial Stability Forum and Institute of International Finance cited in Baker 2008:34; World Economic Forum cited in Lam 2009:22), namely the ability of boards to oversee senior management as well as to understand and monitor business aspects, including a risk management process (National Association of Corporate Directors as cited in McDonald 2009:34). According to these bodies, the failure of risk management is linked to four key elements that are now briefly discussed.

- The governance structures that provide a framework for the responsibilities of the risk management elements:
    - lack of independence of the risk management function with reporting to the chief executive officer or chief financial officer instead of the risk committee and/or board (refer to section 3.3.6.1 on p. 177);
    - many parties are involved in the framework, complicating the governing structure;
    - responsibilities are not properly allocated to various parties and/or certain parties do not take their responsibilities seriously. This usually starts at the top (board and senior management) and works down to the rest of the organisation's employees (refer to section 3.7.1.1 on p. 216); and
    - management's inability to define the risk management framework.
- The methods and techniques used during the risk assessment steps:
    - systems, tools and techniques are not automated, additionally, as the risk management process is a comprehensive and on-going exercise it should be documented, for example, in a risk register (refer to section 3.5.3 on p. 203); and
    - methods used result in too much focus on insignificant risks, for example, regulatory risks that are a result of past problems, and do not always address emerging risks or unexpected events.
- How the output of the risk assessment is incorporated into the organisation's strategies to optimise the risk-return:
    - individual risks are addressed separately with no integration, thus providing a silo approach to risks (refer to section 3.7.1.2 on p. 217);
    - processes focus on past trends instead of current or potential future events;
    - methods are either too qualitative or too quantitative instead of incorporating both methods as needed. This is usually a direct result of the lack of competent, skilled and knowledgeable individuals;
    - ineffective reporting on the performance of the risk management process; and

- the organisational structure's incapability to identify and assess all the relevant and emerging risks.

- The reporting and monitoring processes with regard to the risk management framework:
  - risk reporting is not done on a timely basis;
  - there is a lack of quality information in reports, especially those for senior management and the board;
  - the usefulness of the findings is questioned; and
  - failure to communicate the value of the process to all parties involved.

Although many other factors can also be included in the above list, the literature supports the above as the main reasons for the application of risk management failing to produce results. Also, two of the above factors are highlighted as the most prominent reasons for risk management being either unsuccessfully implemented or not implemented at all. These are briefly discussed.

3.7.1.1 Lack of commitment

A holistic approach to risk management requires a top-down view of risks. Therefore, leadership from senior management and the board to incorporate a risk mindset into the organisation's culture is a critical element to an effective risk management framework. Many argue (Crawford & Stein 2004:503; Beasley *et al.* 2005:529; Borgelt & Falk 2007:125; Berley 2007:25; Campbell 2008:54; Lam 2009:24; Galloway & Funston n.d.:24) that without the buy-in of the board, as the overseers of the framework, and senior management as the initiators of the implementation, risk management cannot be successful. Unfortunately research has indicated that although in many instances management perceive the risk management framework as an excellent tool to assist in managing crucial risks threatening the organisation, it is also sometimes perceived as something that must be done to adhere to applicable codes, laws and regulations (Deloitte & IIA (UK and Ireland) 2003:6; Allegrini *et al.* 2006:846; Arena *et al*. 2006:288; Krell 2006:38; Borgelt & Falk 2007:132; Beasley, Branson & Hancock 2009:30).

The first contributing factor to a successful risk management framework is the independence of the board from senior management. This enhances the overseeing role of the board in ensuring that management is doing their fair share in providing an effective framework (Kleffner *et al.* 2003:60; Beasley *et al*. 2005:529; Beasley *et al.* 2008:44-45). Secondly, the board as well as senior management must be convinced that risk management is adding value to the organisation as a whole (De la Rosa 2007/8:22-23; Ramamoorti *et al.* 2008:57; Moody 2009:75; Beasley *et al.* 2009:30). Thirdly, a significant change of mindset is needed by senior management to embrace a culture of risk management. As information is shared across boundaries, this could be view by many as a breach of confidentiality, or a way to compare different business units and processes. Also, it is perceived by many as being time consuming or a waste of time (Beasley *et al.* 2008:46). Lastly, with the implementation of risk management across the organisation, the idea of dedicated individuals being the sole responsible parties for risk management is changing to make way for the view that all employees should be risk managers. Line management especially should be constantly aware of what the risks are that threaten their sphere of responsibilities and should make their subordinates as well as the risk management structure aware of these (Baker 2008:34). Many risk experts warn (Lenckus 2009:16) that it is not an easy task to convince middle and lower management to support risk management. Therefore, if the board and especially the senior management of the organisation are not pro-risk management by setting the 'tone at the top', to permeate a risk culture or mindset throughout the organisation will be a very difficult task.

3.7.1.2 Risk management (silo approach) *versus* enterprise risk management (holistic approach) resulting in neglecting strategic and/or operational risks

In section 3.5 on p. 191 the difference between risk management and enterprise risk management is explained. When connecting these two concepts to strategic and/or operational risk management, it is evident that a holistic approach will ensure that both these levels are addressed. According to McCarthy and Flynn (2004:131,247), Shenkir and Walker (2006:32) and Griggs (2008:45), operational

risk management and strategic risk management are complementary and highly dependent aspects of risk management. According to the COSO Report (2004:123-124) and Griggs (2008:47), operational objectives are linked to the effectiveness and efficiency of an organisation's activities. Strategic objectives are linked to a high-level goal that supports the vision and mission statements of the organisation. The organisation thus first determines what its strategic plan is, implements the actions needed to achieve this plan, and sets operational objectives for each activity (refer to section 3.5.2 on p. 195 for a discussion).

Without having strategic objectives (and managing the risks that threaten the reaching of these), it would be very difficult to set operational objectives (and manage the risks threatening these). Equally, without managing the risks threatening the operational objectives, the strategic plan will not be fulfilled as the operational objectives feed into the strategic objectives. For an organisation to manage risk and obtain the ultimate balance between risk and return, risk cannot be viewed in sub-sections or silos, but should be viewed in a holistic manner.

One of the lessons learned from the current global financial crisis is that major risk events (the so called 'black swans') do not result from one single risk, but usually from a series of wrong decisions and risks not managed properly (Lam 2009:25). These risks are generally under-managed until they occur, and thereafter over-managed, for example the 9/11 terrorist attack and the current financial crisis (Barton, Shenkir & Walker 2008:24). The answer to this problem is that organisations should integrate their risk management efforts in a holistic approach, focusing on critical interdependencies to broaden management's perspective (Wood & Randall 2004:28; Storey 2009:43; Killackey 2009:29). When corporate strategy is aligned with an enterprise-wide risk management approach, all types of risks can be managed. The only requirement for this to be successful is cooperation amongst executives, managers, line-employees and other role players as well as the commitment of these individuals to the process.

Lastly, according to McCarthy and Flynn (2004:131-147) operational risk management is less well defined as boards and senior management usually focus on strategic risks. It is, however, important for the board and senior

management to understand the consequences of not managing operational risks properly. Most corporate scandals occurred as a result of operational risks not being addressed and managed, especially due to inadequate or faulty internal processes, staff or systems. Although scandals such as Enron, Parmalat and WorldCom all refer to major risk events that caused the downfall of the organisations, it was as a result of operational aspects, and not strategic aspects, gone wrong.

3.7.2 Current trends and new developments

As with any new developing discipline, risk management is facing many changes that influence the current trends. According to the literature, there are numerous new developments within the risk management framework, including risk management approaches and processes. Most of these are discussed in this chapter. The following list is a summary of the most recognised of these new developments:

- Risk management framework including the organisation's structure and leadership:
    - implementing a separate risk committee (Atkinson 2008:42-45; Lam 2009:24);
    - enhancing the risk manager to be considered a leader with other senior executives (Baker 2008:34);
    - developing, approving and communicating a comprehensive risk management policy (Rizzi 2008:5-6; Lam 2009:24; RIMS Risk Maturity Report cited in Minsky 2009);
    - defining the risk terminology (Scanfield & Helming 2008:42);
    - developing executive incentive compensation based on risk-return decisions (Lam 2009:2);
    - rising expectations of all stakeholders with regard to risk management (Meiselman 2007:40; RIMS Risk Maturity Report cited in Minsky 2009); and

- developing a risk culture by embedding risk in strategic and operational activities (Scanfield & Helming 2008:44; Institute of International Finance cited in Baker 2008:35; Killackey 2009:29).

- Risk management process:
  - aligning risk management with existing processes and systems (Baker 2008:34; Griggs 2008:45);
  - using a risk maturity model or other tool to determine risk management quality (Puccia 2007; Liebowitz 2007:3; McDonald 2007:28; Moody 2007:100; Minsky 2009);
  - implementing a holistic risk management process (Meiselman 2007:40; Griggs 2008:49; Charnock 2009:55);
  - establishing a uniform approach by developing a set of methodologies and terminologies for the whole organisation (Baker 2008:34; Rizzi 2008:6-7; Moody 2009:74);
  - deploying technology to assist (Scanfield & Helming 2008:44);
  - including upside risks or the possible loss of opportunity in the risk management process (Ramamoorti *et al.* 2008:54);
  - implementing a risk hotline to assist in identifying risk (Peterson 2006:3-6);
  - training and/or appointing risk qualified professionals (Meiselman 2007:40; Ramamoorti *et al*. 2008:54-55; Moody 2009:74);
  - getting all employees involved and enthusiastic about risk management (Baker 2008:34; Moody 2009:74); and
  - using quantitative risk analysis as opposed to the current qualitative model used by most (Emblemsvag & Kjolstad 2006:401-406; Hespenheide & Funston 2006:13).

Apart from the above list, one trend that is worth mentioning is the current growth in risk management implementation that is anticipated to escalate even further in the future. Although the current global financial crisis, especially the credit crunch in the financial sector, is seen by many as a direct result of the failure of risk management, organisations are admitting that it failed as a result of poor risk structures and systems in place and poor commitment of the board and senior management to risk management. According to various risk consultants, risk

managers and risk experts, now, more than ever, organisations either want to implement risk management, or improve existing frameworks (cited in McDonald 2009:27-35; Lam 2009:22; cited in Hofmann 2009:14). COSO (2009) issued a document to assist the board and senior management in strengthening their risk management efforts. It includes guidance on risk management philosophy, understanding risk management practices, how to review the risk portfolio in relation to the risk appetite, and the identifying of key risk indicators and their related responses.

Lastly, best practices for public sector risk management, as with the private sector, are constantly evolving and, apart from the above list, include a few other aspects worth mentioning (Canada – Treasury Board of Canada Secretariat 2001:2; Dittenhofer 2001(b):474; SA – Public Service Commission 2002:29-30; UK – Cabinet Office 2002(a):75-91; SA – Public Service Commission 2003:26-30; Rowe 2004:52; Crawford & Stein 2004:504-509; Halachmi 2005:303; McPhee 2005:6; Merna & Al-Thani 2005:21-22; Leung & Isaacs 2008:510; Hofmann 2008:15-16; Breighner 2009:20-26):

- The awareness of senior management and politicians of:
  - the cost of not managing risk; and
  - risk management enhancing government's governing, accountability and stewardship responsibilities.
- Apart from assessing the impact and likelihood of risks identified, the seriousness or importance of the risk to the reputation of government must also be considered.
- Greater transparency is needed with regard to risks threatening the general public, the management of these by government, as well as communication of processes followed and results obtained.

3.7.3 Conclusion

Risk management is a relatively new addition to corporate governance. However, it has grown tremendously over the last few years. Critical questions are being

raised as a result of the financial crisis that is currently being experienced worldwide. It seems that more and more organisations' managements and governments have to choose between implementing an effective and efficient risk management framework, or suffering the consequences of further emerging risks.

3.8 SUMMARY AND RELEVANCE TO THE STUDY

The development of corporate governance with specific reference to the concept of risk management is discussed throughout this chapter. This section summarises the aspects most relevant to this study.

Although corporate governance has been practised for a long time, it is only recently that it has evolved to a much debated and discussed concept. To define corporate governance is very difficult, if not impossible, due to the fact that no two organisations operate exactly the same way. Also, the need for a specific corporate governance process or system may differ. The results of the literature regarding these two aspects are summarised below:

- A broad perception of corporate governance is that it is:
  - all process(es) and/or system(s);
  - unique to each organisation;
  - driven by the board and executive management;
  - as they are accountable to various stakeholders;
  - to direct and control the organisation;
  - in the most effective and efficient way possible.
- The need for sound corporate governance principles is linked to:
  - the consistent occurrence and even increase in corporate scandals due to, inter alia, the misuse of various corporate governance aspects;
  - the increased demands of investors' requirements;
  - stakeholders demanding more comprehensive accountability; and
  - principles-driven guidance being more acceptable to the business environment as its 'apply/comply or explain' guidance provides

management with the freedom to regulate the organisation to the best of their abilities, but within certain boundaries.

Risk management is an effective tool that can be used to assist management with their responsibility to address corporate governance principles. The following concepts are required to ensure that risk management and the need for effective risk management are communicated in such a manner that it is understood by all relevant stakeholders:

- As it is a fairly new concept, the terminology used differs from document to document, even so the terms can be defined as:
    - the risk management framework is the totality of all structures, processes, system, methodology and individuals involved to implement a risk management strategy;
    - the risk management process is part of the risk management framework and is explained as the steps followed to identify, assess, treat, monitor and report risks;
    - risk management refers to all systems and processes in place that deal with risks that have an impact on a specific area on a micro level, usually within a specific silo; and
    - enterprise risk management is the extension of risk management that incorporates all systems and processes across the organisation to view risk from a holistic point.
- The need for effective risk management can be linked to aspects such as:
    - the coordination of all risk management efforts, including the alignment of terminology;
    - the proactive management of risks; and
    - the positive effect on investor's decisions.

With regard to what risk management entails and who is responsible, much guidance has been issued and these are constantly being updated:

- Guidance entails formal corporate governance codes and legislation, as well as separate risk management–specific documents.
- The roles and responsibilities include:
    - the board of directors delegating the risk management framework to a risk committee;
    - senior management delegating the daily activities to a chief risk officer and/or risk department; and
    - internal auditing providing assurance and/or assistance to both parties.

Risk management consists of two concepts, with the element of risk distinguishing it from general management activities. Risk management within the business environment is referred to as business risk that should be managed and controlled to ensure that the organisation achieves its objectives. After comparing various risk management process models, it is concluded that the process entails six steps and the outcome should be documented in a proper risk register. The results of the literature study confirm the following:

- Determine the objectives that must be reached, either on a strategic level or on an operational level.
- The identification of risks, including:
    - risk as an uncertainty, risk as a threat and risk as a loss of opportunity; and
    - the level of the risk being either inherent risk (gross risk) or residual risk (net risk after measures have been taken to reduce the risk).
- The assessment of risks identified, including:
    - the possible impact of the risk on the organisation; and
    - the likelihood of the risk occurring;
        - measured in terms of the risk appetite and risk tolerance as determined by the board.
- The treatment of the risk as indicated by the measurement and risk appetite, being accepting the risk, avoiding the risk, reducing the risk by implementing further measurements or sharing the risk with an external party. Further actions could include exploiting opportunities, terminating the

activity that gives rise to intolerable risks and integrating some or all of the above responses.

- The outcome of the risk management must be communicated to all parties that could make a difference.
- The process is ongoing as risk is not stagnant. As new risks emerge, the risk management process should identify them and assure that they are managed accordingly.

Risk maturity is the extent to which the elements within the risk management framework have been implemented effectively and applied within the organisation. A risk maturity model is used to determine the risk maturity levels of a specific organisation compared to best practices. Common criteria used in such a model include:

- the risk management approach including risk management culture, involvement in strategy setting, risk management policy setting and appropriate reporting and communication;
- the risk management process;
- the staff's experience;
- performance management; and
- sustainability.

With regard to the future of risk management, the possible weaknesses in the implementation and application thereof include:

- a lack of commitment of management to the process; and
- a risk management (silo) approach that neglects the holistic view and, as such, may not properly identify many risks, or if they identified, they may not be managed sufficiently.

However, even with these problems it seems that risk management is growing and more and more organisations, especially with the current financial crisis, are turning to risk management to assist in preventing risks from occurring that could

harm the organisation beyond repair. Internal auditing, being one of the key role players in the risk management framework, needs to be in a position to assist management where and as needed. The IIA should provide their members with sufficient and applicable guidance. The role of internal auditing with specific reference to the generic concept of risk is discussed in the next chapter.

CHAPTER 4
THE ROLE OF INTERNAL AUDITING WITH SPECIFIC REFERENCE TO RISK

4.1 INTRODUCTION

The evolution of corporate governance as discussed in the previous chapter, with emphasis placed on the increase in management's responsibility and accountability within the business environment, has forced management to revisit the roles and responsibilities of various parties related to these concepts (Coupland 1993:4; Dallas 2004:14; Van Gansberghe 2005:69; Merna & Al-Thani 2005:53; Gendron, Cooper & Townley 2007:105). One of these parties is the internal audit function. At the same time the internal audit profession has realised that it will have to adapt to the changing environment in which it operates (refer to sections 2.4 on p. 70, 2.5 on p. 84 and 2.6 on p. 113). A statement made by PWC (2008(b)) after a study performed on the perceived status of internal auditing in 2012 concludes:

> The rapid growth of the profession and the many changes in the business environment makes [*sic*] it essential for the internal audit profession to adopt new mindsets if it wants to remain a role-player in the future.

Many studies (Arena *et al.* 2006:288; Allegrini *et al.* 2006:849-852; Roffia 2007:12-14; IIA Research Foundation 2007:344-351; Ernst & Young 2008:2; PWC 2008(b):31-39; IIA Research Foundation 2009(a):1) addressing the new trends in the internal audit profession as well as what the future holds include the expansion of its role in corporate governance aspects, and more specifically, risk-related aspects. For internal auditors to be able to add value to these two areas it is vital that they have sufficient knowledge of the business in general and its strategies, as well as skills in risk analysis (IIA Research Foundation 2007:283-284). However, only 27% of respondents to the IIA Research Foundation's 2007 study indicated that they are involved in the strategic frameworks of their

organisations and only 23% with aligning strategy with performance (IIA Research Foundation 2007:347).

For internal auditing to truly add value in the field of corporate governance and risk management, internal auditors will have to be aware of the potential effect they can have on these areas and align their activities in such a manner that management will take note of their output. In this chapter, the role of internal auditing in corporate governance is briefly discussed. Thereafter, the influence of risk on the internal audit function's activities is debated, with specific reference to performing a risk-based internal audit assurance engagement.

4.2 CORPORATE GOVERNANCE AND INTERNAL AUDITING

As risk management and internal auditing are both elements of sound corporate governance principles it is important to discuss the literature addressing the responsibilities of the internal auditor with regard to corporate governance structures and processes. This section first briefly mentions the guidance provided by the IIA, where after the roles and responsibilities of the internal audit function are discussed.

4.2.1 Guidance on corporate governance by the Institute of Internal Auditors

As mentioned before (refer to sections 1.2.4.1 on p. 9 and 2.4.4.1 on p.81), the formal guidance published by the IIA Inc., namely the IPPF, consists of six elements with some being mandatory and others strongly recommended. These and other relevant IIA guidance are discussed in the context of the role of the internal auditor with regard to corporate governance processes.

4.2.1.1 International Professional Practices Framework – *Standards* and practice advisories

According to *Standard* 2100 (IIA 2009(a):27), the nature of the internal audit work performed must include the evaluation and contribution to the improvement of

governance processes. *Standard* 2110 (IIA 2009(a):27-28) built on this by identifying specific tasks, for example, assessing and recommending improvements, as well as specific areas, for example, ethics and values, performance management and accountability, to name the most important. Various practice advisories provide further guidance to the members that, although not mandatory, are 'strongly recommended'.

4.2.1.2 International Professional Practices Framework – Organisational governance: guidance for internal auditors

The IIA (2006(b)) has issued a position paper to complement the *Standards* and practice advisories with regard to the activities that internal auditing should perform on corporate governance. As with the risk management maturity levels (refer to section 3.6 on p. 205), the maturity of the governance processes and systems will have an effect on the role that internal auditing could play; from a more advisory role in less mature organisations, to focusing on evaluating the effectiveness, analysing the level of transparency, comparing with best practices and identifying compliance with governance codes. The document lists a few of the most important areas within the governance structures where internal auditing should be involved, as well as other participants and organisational initiatives that have an impact on corporate governance.

4.2.2 Roles and responsibilities

It is important to note that not all governance structures and processes are auditable (Marks 2007:32) – either as a result of the internal audit function not being able to add value due to the type of activities, or as a result of the board and management not allowing the internal auditors to perform certain duties.

According to research studies, the key elements of the role played by modern internal auditing in governance can be summarised as follows (Leung *et al.* 2003; KPMG 2003(b):2; Gray 2004:17-19; Gramling *et al.* 2004; Crowe Chizek 2005:5-11; ECIIA 2005:35-38; Staciokas & Rupsys 2005:173-174; Crowe Chizek 2006:7; Marks 2007:32):

- assisting the board of directors and audit committee in performing their duties and responsibilities;
- adding value by providing an independent and objective assurance of activities to top management (chief executive officer, chief financial officer, audit committee and risk committee);
- investigating certain governance activities and structures, for example, the board structure, objectives and dynamics, tone at the top, etc.;
- reviewing the effectiveness of business practices and ethical aspects;
- identifying fraud indicators;
- reviewing operational and financial performance;
- verifying information used by management to make decisions;
- providing advice on various aspects to different levels of management;
- assessing the accomplishment of objectives;
- assisting with disclosure of information and transparency aspects;
- assisting management with the risk management framework;
- monitoring corporate governance activities and compliance with organisational and external policies;
- evaluating the risk and control frameworks, including the control culture; and
- facilitating and enhancing communication and coordination with various role players within the organisation, for example, the risk department, and externally, for example, the external auditors.

Paape *et al.* (2003:253-254), Gramling *et al.* (2004:194-195), Goodwin-Steward and Kent (2006(b):93), CBOK (IIA Research Foundation 2007:191-194) and Deloitte & IIA (UK and Ireland) (2008:8) provide proof that the existence of an internal audit function is positively associated with corporate governance quality, especially when an organisation has an independent audit committee and/or board. Furthermore, a study performed by Roffia (2007:7) indicates that 92% of respondents (chief audit executives in listed Italian companies) do perform corporate governance audit activities. The CBOK study (IIA Research Foundation 2007:200,209,212) concludes that the internal audit function's activities include the evaluation of management's effectiveness (48.5% of the respondents), ethics

audits (47.1% of the respondents) and social sustainability audits (40% of the respondents). In 51.4% of the respondents' organisations, internal auditing has the responsibility to monitor the adherence to corporate governance and regulatory code requirements. Most respondents (73.3% and 53.2% respectively) indicated that their organisations do have a code of ethics as well as a corporate governance code.

With regard to the future, studies indicate that the role that internal auditing currently plays in governance may increase over the next few years. For example, 75% of the chief audit executives responding in the Deloitte and IIA (UK and Ireland) (2008:8) study foresee that internal auditing will provide considerable value regarding governance processes, compared with only 40% in the previous study (Deloitte & IIA (UK and Ireland) 2003:6). This is confirmed in the results of a similar study (PWC 2008(b):22) where the future impact of corporate governance on the internal audit function's roles and responsibilities is predicted by 84% of the respondents to be moderate to very strong.

The above statistics could imply both a positive and a negative effect on the internal audit profession. On the positive side, internal auditors are recognised by the top structure of organisations for the role they can play in corporate governance. It could be argued that the board and senior management are accepting internal auditing as a major part of sound governance. On the other side, the possible danger for internal auditing in providing assurance on corporate governance processes is that the internal audit function may spend too much time and resources on auditing non-core activities that will not optimally add value as described by the formal internal audit definition. This could lead to the function not having the capacity to perform their other duties and thus possibly neglecting to provide assurance on the areas of risk management and control (refer to figure 2.2 on p. 74 for the three crucial areas covered by modern internal auditing). For example, a study performed by Sarens and De Beelde (2006(a):73) indicates that the adherence to SOX, an initiative to enforce corporate governance on USA organisations, takes up to 50% of the responder organisation's internal audit resources. However, it seems that as organisations become more at ease with the concept of corporate governance, the time spent by internal auditors

providing assurance on corporate governance processes is reducing. Studies performed by PWC (2008(a):35) over the last four years indicate a steep decline in this type of audits (from 2004 – 71% to 2007 – 27%) leaving internal auditing with more capacity to focus on other areas of concern.

4.2.3 Conclusion

The above discussion indicates that internal auditing is firmly on the front line when it comes to corporate governance aspects. The debate about whether the audit of corporate governance processes is adding value to the organisation as per the current internal audit definition or not, will most probably continue. Management has a responsibility to align the corporate culture, structures, processes and systems with best practices and what is best for the organisation, therefore ensuring that the organisation has a sound foundation, which the rest of the activities can build on. Internal auditing should provide management with assurance that their policies and procedures are implemented in practice and/or assist them by consulting on how to establish or improve governance systems. Unfortunately this means allocating valuable internal audit resources to perform these engagements, resulting in less time for the function to perform other tasks.

Traditionally, internal auditors were seen as control experts, thus mainly providing assurance of and input to control systems. Whether this is the optimal allocation of internal audit expertise and knowledge in the modern business environment is debatable. The questions that should be asked by every organisation's management are, what is the best governance philosophy for the organisation to ensure a sound foundation, what is needed to ensure that it is being adhered to, including whether internal auditing has a role to play, and, if so, what that role should be. This includes the role of internal auditing in risk management.

4.3 RISK AND INTERNAL AUDITING

Most parties involved in the business environment recognise that the responsibility for risk management lies with the board and senior management for private sector organisations (IOD 2002:81-82; COSO 2004:83-84; IIA 2004), and

the accounting officer for the SA public sector (SA – PFMA 1999:S38(1)(a)(i); SA – MFMA 2003:S62(1)(c)(i)). To manage risk efficiently and effectively, management should have an understanding of the concept of risk in general and of the specific risks that threaten the organisation in particular, and then establish a proper risk management framework to mitigate risks (IOD 2002:84; Spira & Page 2003:643; Beasley *et al.* 2005:530).

Internal auditors are in the ideal position to assist management with this task as they should, to be able to perform their duties with proficiency and due professional care (IIA 2009(a):18-21), have an overall understanding of how the organisation operates, including the risks threatening the organisation. For example, as they are traditionally seen as the control experts (Sawyers *et al*. 1996:78; Ramamoorti 2003:8), the optimal implementation of controls is directly linked to the risks that they should address. They should thus combine their broader knowledge of the business with their role of assisting management in minimising risks, while still retaining their independence from the business activities and structures (Spira & Page 2003:653; IIA 2004; Fraser & Henry 2007:406). Lubbe and Van der Merwe (2007:25) argue that there are many other reasons why risk management and internal auditing should be aligned, including to provide the board with an accurate risk profile, to assist internal auditing on focusing on high-risk areas, to save cost and to improve efficiency and effectiveness of information, to name the most important.

Although numerous underlying factors will contribute to the role of internal auditing with regard to the management of risk, the most important one is the risk maturity of the organisation (refer to section 3.6 on p. 205 for a detailed discussion). Internal auditing will first have to establish what the organisation's risk maturity is – the more relevant activities and elements of the risk management framework have been implemented effectively, the more risk mature the organisation is (IIA (UK and Ireland) 2003; IIA 2004; De la Rosa 2008(b)). The risk maturity of the organisation will thus form the basis for the role that internal auditing could play regarding risk. For example, if an organisation is risk immature and does not have a proper risk management framework in place, internal auditing will not be able to audit the processes and structures, or

incorporate risks identified by the framework into their daily activities, but would rather advise management on implementing a formal framework.

As briefly mentioned in section 1.7.3 on p. 34, the *Standards* and practice advisories of the IIA (2009(a)) address three specific areas where the internal auditor should play a role regarding risk or incorporate risk into their activities. As the formal guidance of the IIA should be a starting point for internal auditors when performing their duties, this section will focus on these areas. The areas, discussed in more detail below, are the formal risk management framework including the risk management process, the annual plan of the internal audit function's activities based on risk (internal audit risk assessment), and incorporating risk into individual audit engagements (risk-based internal auditing).

4.3.1 Risk management

As discussed in section 3.3.1 on p. 153, risk management consists of two broad principles, namely the risk management framework, and its included risk management processes. The framework is the structures, processes and systems that management establishes to ensure that their risk philosophy is incorporated into the daily activities of the organisation. This refers to numerous tasks and activities, including a risk management process (refer to section 3.5 on p. 191) that could be either comprehensive or partly implemented. With regard to the role and responsibilities of internal auditing in risk management, the discussion below either specifically refers to a risk management framework, a risk management process, or generally to risk management, which includes both.

4.3.1.1 Guidance on risk management

Many books and other literature are available on the topic of the role of internal auditing and risk management. As this study addresses a side addition of risk management, namely the incorporation of risk into internal audit engagements, the guidance discussed is limited to those provided by the IIA and promulgated in SA.

4.3.1.1.1 Guidance by the Institute of Internal Auditors Incorporated

The guidance provided by the IIA is divided between general guidance (*Standards* and the practice advisories), specific guidance in the form of a position paper, and guidance for the public sector.

- **International Professional Practices Framework – *Standards* and practice advisories**

According to *Standard* 2120 (IIA 2009(a):28-29) the internal audit function must evaluate the effectiveness of the risk management process. *Standard* 2120.A1 (IIA 2009(a):29) elaborates on this with specific reference to risk exposures relating to organisational governance, operations and information systems, *Standard* 2120.A2 (IIA 2009(a):29) deals with the risk of fraud, and *Standard* 2120.C3 (IIA 2009(a):29) provides guidance for assisting management with the establishment or improvement of a risk management process. Various practice advisories, that are not mandatory, provide further guidance on this topic.

According to Practice Advisory 2120-1 (IIA 2009(a):107-110), the ideal role for internal auditing is to verify the adequacy of the risk management process(es) – that is, verify whether management has planned and designed the process in such a manner that it provides reasonable assurance that the organisation's objectives and goals will be achieved. The scope of the involvement of internal auditing in the risk management process will be determined by the expectations that the board and senior management have of the internal audit function and may vary from:

- no role in the process;
- auditing the risk management process;
- actively, and on a continuous basis, being involved; or
- managing and coordinating the process on behalf of management, but not taking responsibility.

Although it is suggested that elements of the risk management framework should be investigated in order to form an opinion on the adequacy of the risk

management processes, no mention is made of internal auditing being involved in the overall risk management framework – either by providing input into the risk philosophies, risk policy, structures such as a risk committee and risk department, and the embedding of risk into the day-to-day activities of the organisation, or providing management with assurance. This is a gap in the IIA guidance on the internal audit function activities, and although the IIA's position paper on corporate governance (2006(b):14-15) does refer to the role that internal auditing should play in governance structures, including enterprise risk management as an organisational initiative impacting on governance, it does not specifically stipulate that internal auditing should be providing assurance on the effectiveness and efficiency of the framework. As debated in section 3.7.1 on p. 214, the lack of commitment from management's side to risk management could possibly be one of the reasons for the current financial crisis. Therefore, it is crucial for internal auditing to not only provide assurance on and input into the risk management process, but the overall risk management framework.

- **International Professional Practices Framework – Role of internal auditing in enterprise-wide risk management**

The IIA (2004) issued a statement to compliment the *Standards* and practice advisories on the role of internal auditing regarding risk management. The document suggests the idea of internal auditing playing a core role in providing assurance on the risk management process, providing assurance that risks are evaluated correctly, evaluating the risk management process, evaluating the reporting of key risks, and reviewing the management of key risks. Figure 4.1 on p. 237 summarises the position statement, separating what is sound internal audit practice (blue) from activities that are not appropriate to internal auditing's tasks (red). The middle section (legitimate roles with safeguards) refers to consulting activities that the internal auditor may undertake. As with the *Standards* and practice advisories, although the middle section refers to a risk management framework in terms of maintaining and developing it, it does not include the providing of assurance under the core roles (blue).

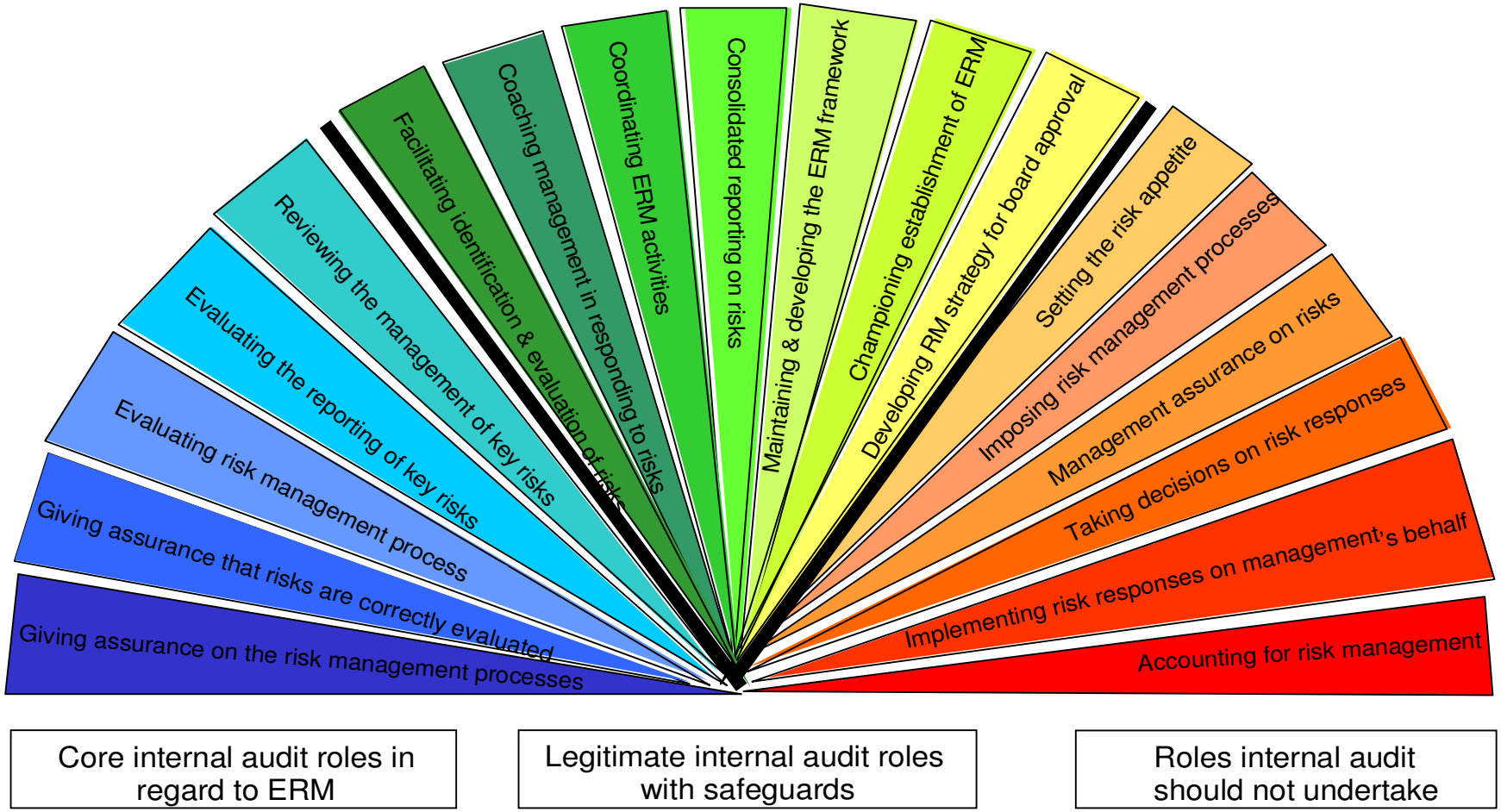


Figure 4.1: IIA position statement on internal auditing's role in Enterprise Risk Management

Source: IIA 2004:2

- **Institute of Internal Auditors Research Foundation – Internal audit capability model for the public sector**

After comprehensive research, the IIA Research Foundation (2009(d)) has developed a capability model, based on the SEI model (Ziegenfuss 2010:68), for public sector internal auditing. The model was developed to assist internal auditors and other internal audit stakeholders in identifying the fundamentals needed for an effective internal audit function within a government structure and the broader public sector (Ziegenfuss 2010:68). With regard to risk management, for government organisations to be on level four of the five-level capability matrix, internal auditing must provide overall assurance on, *inter alia*, risk management.

4.3.1.1.2 South African guidance

The requirements for the role of internal auditing with regard to risk management are similar for both the private and the public sector. The second King Report (IOD 2002:76) stipulates that an assessment of the risk management processes in place within the organisation must be conducted on an annual basis. Internal auditing should assist in the monitoring of the processes. The third King Report (IOD 2009:79-80) elaborates on the above. Specific interesting additions include the reference to providing assurance on the effectiveness of risk management (process and framework), commenting on the level of risk maturity (refer to section 3.6 on p. 205), and incorporating both risk management (silo approach) and enterprise risk management (holistic approach) as discussed in sections 3.5 on p. 191 and 3.7.1.2 on p. 217.

For the public sector, legislation (SA – MFMA 2003:S165(2)(b)(iv)) prescribes that the internal audit function in a local government organisation should advise management and report to the audit committee on the matter of risk management. Although vague, it incorporates the possible providing of assurance on the risk management framework.

The National Treasury has issued an internal audit framework for all government organisations. It stipulates that the internal audit function is responsible for

providing assurance on the adequacy and effectiveness of risk management (SA – National Treasury 2009(b):21) and identifies key objectives that must be met.

4.3.1.2 Influencing factors

Studies exploring the role of internal auditing with regard to risk management (McNamee & Selim 1998:13; Spira & Page 2003:656-657; Allegrini & D'Onza 2003:198-199; Baker 2004(a):17; Beasley *et al.* 2005; Sarens & De Beelde 2006a:73-75; Gramling & Myers 2006:52-58; Roffia 2007:9; Fraser & Henry 2007:403; Deloitte & IIA (UK and Ireland) 2008:8; PWC 2008(a):9; Ernst & Young 2008:5-6; IIA Research Foundation 2009(a):9; Castanheira *et al.* 2010:89-94) all indicate the growth of the implementation of risk management by organisations. The studies also indicate that there is an increasing demand for internal auditing to be involved in risk management. This involvement varies from taking responsibility for the risk management process (not allowed according to figure 4.1 on p. 237), to auditing the risk management process as part of the internal audit annual plan, or actively and continuously supporting and being involved in the risk management process in a consulting role. The latter involves participation in risk committees, monitoring activities, status reporting, and managing and coordinating the risk management process. However, most studies do not refer to internal auditing providing assurance on the overall risk management framework, except for the recent study published by the IIA Research Foundation (2009(a)) on the trends for the profession in 2009 and beyond. In this study, the audit universe (IIA Research Foundation 2009(a):9-10) includes the overall effectiveness of risk management within the organisation's risk environment, referring to both the risk management framework and the risk management process.

When investigating whether the activities performed by the internal audit function are in line with the guidance of the IIA, the evidence is contradictory. For example, the study performed by the IIA Research Foundation (cited in Gramling & Myers 2006:54), where 87% of the respondents indicated that they do have a risk management process in place, identifies that the following core activities are to a large extent being performed by the internal audit function:

- giving assurance on the risk management process;
- giving assurance that risks are evaluated correctly;
- evaluating the risk management processes;
- evaluating the reporting of key risks; and
- reviewing the management of key risks.

Although the study (Gramling & Myers 2006:55) indicates that the respondents do perform the activities as suggested by the IIA (refer to figure 4.1 on p. 237 – blue or legitimate activities), there are a few activities performed (Gramling & Myers 2006:56) that are in contrast to what the IIA suggests (refer to figure 4.1 on p. 237 – red or inappropriate activities), namely:

- setting the risk appetite;
- imposing risk management processes;
- providing management assurance on risks;
- making decisions on risk responses or implementing risk responses on behalf of management; and
- being accountable for risk management.

Sarens and De Beelde (2006(b):238) as well as PWC (2007:15) confirm this tendency. In the latter study, 32% of the respondents indicated that internal auditing is responsible for the risk management process. This is in total contrast to sound corporate governance principles and the guidance provided by the IIA to their members, where internal auditors could facilitate or manage the risk management process (refer to figure 4.1 on p. 237), but should never take ownership of, or be responsible for, the identification, measurement or management of the risks identified. The board must still take final responsibility for these activities.

With regard to the public sector, a study performed in Europe (Castanheira *et al.* 2010:92) identifies that although internal auditing plays a proactive role in the implementation of risk management, it has no further involvement after the framework has been established. Hepworth (2004) asks the question whether the

modern approach to internal auditing based on risk is appropriate for developing counties. He argues that the definition of internal auditing is based on the assumption that reasonable assurance can be provided. In developed countries the public sector is well structured, systems are developed and public servants are properly trained – it is thus easier for internal auditing to provide assurance. This may not always be the case in a developing country. This view is supported by Lutta and Ogwel (cited in Baker 2005:47) who were members of the task team assisting a Kenyan government department in developing a risk-based internal audit plan. Both stipulate that management and internal auditing must first understand the underlying concepts related to risk and risk management before a proper risk management process can be implemented. To be able to reach this goal, public servants must be trained in the use of risk methodology and the risks threatening government organisations must be extensively researched.

4.3.1.3 Conclusion

The above guidance, general information and statistics indicate that the role of internal auditing with regard to risk management is increasing. The IIA has provided guidance to their members with regard to the risk management process, but not on the overall risk management framework. However, it seems that this is an area that is a new trend for internal auditing, thus guidance is needed. Additionally, although the IIA has provided definitive guidance on the activities that may be performed by internal auditors *versus* what is inappropriate, studies indicate that IIA members do not always adhered to these rules. The guidance clearly stipulates what are assurance activities (figure 4.1 on p. 237 – blue), what are consulting activities (figure 4.1 on p. 237 – green) and what are inappropriate activities (figure 4.1 on p. 237 – red). To protect their independence and objectivity, internal auditors need to follow this guidance more carefully. Finally, although it seems that most organisations and their internal auditors are implementing some form of risk management activities, the knowledge and competencies needed are not necessarily on the level that they should be. Internal auditors should first ensure that they are 'risk-wise' and thereafter provide management with appropriate guidance to uplift the overall risk management capabilities of the organisation.

4.3.2 Annual planning of the internal audit function's activities

Risk management is becoming more important to organisations, internal auditing is being recognised as one of the parties that could assist with this, and the IIA is providing the necessary guidelines to internal auditors regarding this matter. The next step for the internal auditor will be to align the outcome of the risk management process (list of risks threatening the organisation) with the activities of the internal audit function. Apart from performing an internal audit assurance engagement on the risk management framework and/or the risk management process, internal auditors should incorporate the outcome of the risk management process into their internal audit annual plan. This is also referred to as risk assessment or macro assessment of risk (McNamee 1998:71; McNamee & Selim 1998:49-50; Allegrini & D'Onza 2003:197; Spencer Pickett 2006:107). To avoid confusion with the risk assessment step in the risk management process (refer to section 3.5.2.3 on p. 198), this macro process will be referred to as internal audit annual planning and, when referring to assessing risk as part of the process, it will be referred to as internal audit risk assessment.

Internal auditors are often criticised for focusing on the past. They give advice and make recommendations based on the examination of historical transaction records and the historical workings of the internal control system (Sawyer *et al.* 1996:6-7; Anderson 2003:99; Spira & Page 2003:646). For internal auditors to add more value to the organisation, and meet the rising and changing expectations of all their stakeholders (Spencer Pickett 2006:20-22; PWC 2008(a):3; Deloitte & IIA (UK and Ireland) 2008:10), a shift in emphasis must be made from the past to the future. If internal auditors focus on present and future risks, there is a much better chance that they will address all the matters that management is concerned about (Nagy & Cenker 2002:131; Anderson 2003:100-101; Deloitte & IIA (UK and Ireland) 2003; Spira & Page 2003:647-649).

The scope of this study does not include the internal audit annual planning process that has to be performed by the chief audit executive. However, for the sake of completeness, this process as well as the link with the formal risk management process will be discussed briefly.

4.3.2.1 Guidance on internal audit annual planning

As with the previous section, only guidance provided by the IIA and other relevant SA guidance is discussed.

4.3.2.1.1 Guidance by the Institute of Internal Auditors Incorporated

The audit universe (Spencer Pickett 2006:114-115; IIA 2009(a):93) is a list of all possible auditable engagements that could be performed within an organisation and includes both strategic as well as operational activities. It is usually impossible to perform all these engagements due to resource limitations. Therefore, according to *Standard* 2010 (IIA 2009(a):25-26) and Practice Advisory 2010-1 (IIA 2009(a):93-94), the chief audit executive should base the internal audit function's plan on a risk assessment that is performed at least annually. Factors influencing this planning based on an internal audit risk assessment include components of the organisation's strategic plan, outcome of the risk management process, input from senior management and the board, to name but a few.

Two additional practice advisories (IIA 2009(e) and IIA 2009(f)) addressing this area have been developed by the IIA. The first document (IIA 2009(e)) acknowledges the fact that the information obtainable through the risk management process is crucial in developing the internal audit function's annual plan. The document concludes that the plan should focus on (IIA 2009(e):par 15):

- unacceptably high residual risks where management's attention and action is urgently required;
- unacceptably high inherent risks;
- controls that mitigate the inherent risks to acceptable levels; and
- areas where the differences between the inherent and residual risks are high.

The second document (IIA 2009(f)) recommends that the chief audit executive should minimise duplication of effort by coordinating the activities of the function with other internal and external providers using assurance maps identifying all the crucial areas and the responsible parties (IIA 2009(f):par 8). These include (IIA 2009(f):par 4) various levels of management, external auditors, expert auditors, other bodies and/or committees such as quality assurance, risk management, etc.

4.3.2.1.2 South African guidance

Both the private sector (IOD 2002:90) and the public sector (SA – National Treasury 2005:3.2.7, 2009(b):17) stipulate that the internal audit function must prepare a strategic audit plan based on its assessment of key risk areas for the organisation. According to the third King Report (IOD 2009:94), internal auditing should plan its activities according to risks threatening the organisation, and taking into consideration the needs and expectations of key stakeholders. The Treasury Regulations (SA – National Treasury 3.2.7(a), 27.1.8) elaborates on this process as it stipulates that the internal audit function must prepare a rolling three-year internal audit plan based on the assessment of key risk areas, taking into account current operations, the strategic plan and the risk management process. For the local government organisations, the MFMA (SA – 2003:S165(2)(a)) stipulates that the internal audit function must prepare risk-based audit plans for each financial year.

4.3.2.2 Influencing factors

More internal audit functions are using risk methodologies to plan their activities (Allegrini & D'Onza 2003; PWC 2008(a):16; Castanheira *et al.* 2010:88-94) and it seems that this tendency is growing (PWC 2008(b):31). If a formal risk management process is in place within the organisation, it is important for the internal audit function to consider the output of such a process in drawing up the annual plan, for example, does the annual plan cover the strategic high-risk areas to be audited within the foreseeable future (Spencer Pickett 2006:7; PWC 2008(a):16-18). By using the output of the risk management process in the

planning of the internal audit function's activities, it is possible to ensure that the most important auditable areas within the audit universe are focused upon.

Study results concerning the use of the risk management process's output (management's responsibility to identify high-risk areas) in the internal audit annual plan are contradictory. Some studies indicate (Ernst & Young 2007:10; PWC 2007:12; PWC 2008a:18) that it is used as guidance when planning the internal audit function's activities, while others (Allegrini & D'Onza 2003:197; McCuaig 2006:4; Arena *et al.* 2006:287; Sarens & De Beelde 2006(a):76) indicate that organisations do not use this valuable source of information. Castanheira *et al*. (2010:91-94) identify certain factors influencing the tendency to use this approach, namely the size of the organisation (larger organisations have a greater tendency), type of industry (finance organisations tend to have the highest tendency), the sector (the private sector has a greater tendency), globalisation (international organisations have a greater tendency), and listing on a stock exchange (listed companies have a greater tendency). 83.7% of the respondents in the CBOK study (IIA Research Foundation 2007:116) indicated that they adhere to the guidance on how to manage the internal audit function, including the annual plan based on a risk assessment, and 28.3% (2007:223) indicated that they extensively use a specific audit tool or techniques to perform this task.

The study performed by Ernst & Young (2007:10) identifies a problem that could be linked to the inappropriate and ineffective planning of activities by the internal audit function. Chief audit executives world-wide indicated that they (only 21% completed the entire internal audit annual plan and 24% completed up to 80%) struggle to complete the internal audit annual plan due to various reasons, including personnel shortages and not focusing on the crucial aspects identified by management. For the latter, using internal audit risk assessment to determine these aspects is vital.

PWC (2008(a):3,16-18) highlight the importance of internal auditing focusing on strategic, operational and business risks in addition to financial and compliance risks as a new trend for the profession. The reason for this shift from the

traditional focus on the latter is that 80% of loss in external shareholders' value could be linked to strategic, operational or business risks. In spite of this statistic, only 24% of the Fortune 500 participants in the study (PWC 2008(a):16) indicated that the internal audit function's risk assessment process is linked to the outcome of the risk management process that has as its main objective to identify strategic, operational and business risks.

4.3.2.3 Conclusion

From the above discussion it is clear that a properly structured internal audit risk assessment, incorporating the outcome of the risk management process, can be used to assist the internal audit function in allocating scarce resources to investigate the strategic high-risk areas of the organisation. This way of adding value to the organisation can be further supported by incorporating a risk-based audit approach when performing a specific audit engagement.

4.3.3 Internal audit engagements

Risk-based internal auditing expands on the risk management and internal audit risk assessment processes by shifting the vision of an internal audit engagement. Although the *Standards* refer to two types of engagements, namely an assurance engagement and a consulting engagement (refer to section 2.4.1.1 on p. 71 and figure 2.2 on p. 74 for a discussion), this section will only focus on assurance engagements. In the literature (McNamee 1998:71; McNamee & Selim 1998:103; Allegrini & D'Onza 2003:198; Spencer Pickett 2006:143; Castanheira *et al.* 2010:79) risk-based internal audit engagements are also sometimes referred to as risk assessments or micro risk assessments. In order not to confuse this risk assessment with the risk assessment step in the risk management process (refer to section 3.5.2.3 on p. 198), as well as internal audit risk assessment as discussed in section 4.3.2 on p. 242, this will be referred to as an internal audit risk-based engagement or when referring to the risk assessment, internal audit engagement risk assessment. This methodology is investigated in greater depth in section 4.5 on p. 258 and is only briefly introduced here.

When performing an internal audit engagement, instead of assessing the business activities within the framework of the internal control system ('control paradigm'), the business activities are viewed within a framework of risk ('risk paradigm'). The internal auditor's focus moves from identifying and testing internal controls, to the manner in which management addresses and manages risks – this would probably include internal controls. Furthermore, the internal auditor should, while performing the preliminary investigation of the internal audit engagement, or during the performance of the engagement, identify additional risks that are threatening the organisation's ability to achieve its objectives. In this way, internal auditing, true to the definition of the profession, could add more value in making sure that the organisation's objectives and goals are met, thus also assisting management. This is directly in line with good corporate governance practice.

The current global growth in internal auditing (refer to table 1.1 on p. 7) where practicing internal auditors are becoming more aware of the IIA *Standards* and other guidelines, as well as the scarcity of competent internal auditors (refer to sections 1.2.3 on p. 8 and 2.6.3 on p. 119), the many changes within and the challenges faced by the profession (refer to sections 2.4 on p. 70 2.5 on p. 84 and 2.6 on p. 113), and the changes in the business environment all mean internal auditors have to adapt by performing their duties more effectively and efficiently. Correctly used, risk-based internal audit engagements can be of great assistance to the internal auditor in overcoming this challenge.

4.3.3.1 Guidance on internal audit engagements

As with the previous section, only guidance provided by the IIA (both Inc. and UK and Ireland) and other relevant SA guidance is discussed. Further guidance, where applicable, is incorporated in the discussion in sections 4.4 on p. 251 and 4.5 on p. 258.

4.3.3.1.1 Guidance by the Institute of Internal Auditors Incorporated

According to *Standards* 2200, 2201 and 2210.A1 (IIA 2009(a):31-32), when planning an internal audit engagement, internal auditors must consider the significant risks to the activity under review, as well as the adequacy and effectiveness of the risk management process(es) that resides within the scope of the engagement. Practice Advisory 2210.A1-1 (IIA 2009(a):125-126) elaborates on this by identifying certain tasks that the internal auditor should perform, namely:

- The internal auditor should consider the risk assessment performed on the activity under review (refer to section 3.5.2.3 on p. 198), with specific reference to the:
  - reliability of the assessment;
  - process(es) in place with regard to the monitoring, reporting and resolving of risk aspects;
  - reporting structures and responses when risks exceed the risk appetite limits; and
  - risk in activities related to the activity under review.
- If needed, the internal auditor should perform a survey to obtain information on the activities, risks and controls.

Practice Advisory 2200-2 (IIA 2010) also refers to a risk-based internal audit engagement with the emphasis placed on the fact that internal auditors should identify the key controls mitigating the significant risks of the organisation as a whole, instead of only the risks affecting the activity under review.

4.3.3.1.2 Guidance by the Institute of Internal Auditors (UK and Ireland)

The IIA (UK and Ireland) has issued a position statement on risk-based internal auditing (2003), discussing the fact that the focus of internal auditing has shifted. A structured approach is presented with risk maturity determining how internal

auditors could use the approach in either a risk mature or risk immature organisation.

4.3.3.1.3 South African guidance

Not much guidance is available on this topic in SA. The third King Report (IOD 2009:94-95) includes risk-based internal auditing concepts as a lengthy addition to the second report. It urges the internal audit function to take note of the organisation's assessment of strategic, financial, operational, compliance and sustainability risks when performing its annual planning. Although it does not specifically mention risk-based internal audit engagements, it could be assumed, by implication, that the guidance also refers to risk being included in the execution of an engagement.

According to the Treasury Regulations (SA – National Treasury 2005:3.2.6, 2009(b):24), all internal audit engagements in public sector organisations must be performed according to the IIA's *Standards*, thus including risk-based internal auditing.

4.3.3.2 Influencing factors

After a comprehensive search, it seems that not much research information is available on the performance of a risk-based internal audit engagement. According to Allegrini and D'Onza (2003:198), most internal auditors still follow the control paradigm and as such do not see including the identification of risks when planning the audit engagement as crucial (only 67% of the respondents perform some form of risk-based internal audit engagements). This is echoed by a study performed by Castanheira *et al.* (2010:95) with only 31% of respondents indicating that they take a risk-based approach during an internal audit engagement. The study performed by PWC (2008(a):4-5) suggests that the audit committee is setting higher performance standards for internal auditing. This includes shorter audit cycle times (from the commencement to completion of an audit engagement) due to the rapid changes within the business environment. The follow-up study (PWC 2008(b):34-35) on the future of the profession

underlines this fact by urging internal auditors to move beyond a cyclical and static audit approach and conduct internal audit engagements on a more targeted basis responding to specific risk concerns. Focusing on mainly the high-risk areas within a specific engagement should shorten the audit cycle time as fewer audit procedures will be performed (for example, low-risk areas could be excluded). A study performed by Deloitte (2005:9) amongst 800 executive members on the state of their organisations' control programmes, compliments the move to a risk-based internal audit engagement approach. With regard to the control programme in their respective organisations, 56.3% indicated that over-controlling on routine areas is a huge cause for concern, 29.1% indicated insufficient controls in high-risk areas and 32.2% indicated insufficient focus on high-risk areas in audit programmes. Only 13.9% indicated that their control programmes are lean and balanced. The newly developed practice advisory (refer to section 4.3.2.1.1 on p.243) supports this by suggesting that internal auditors should identify unnecessary, redundant, excessive or complex controls that do not mitigate risk effectively and efficiently (IIA 2009(e):par 10).

Various studies and other literature based on risk and the external audit profession (Eilifsen, Knechel & Wallage 2001; Houck 2003; Sutton & Hampton 2003; Curtis & Turley 2006; Knechel 2006; Prinsloo 2008) define risk-based auditing as an audit where the efforts are focused on areas of higher risks. They all urge external auditors to make use of this methodology, arguing that after all the corporate scandals where auditors were involved, a new way of thinking is needed. The higher risk areas are usually the most crucial to be addressed in order for the organisation to achieve its objectives and goals. Thus, by using this type of audit methodology, both the client and the external audit firm should benefit. This could be the same scenario for the internal audit profession.

4.3.3.3 Conclusion

In contrast to the research information available on the role of internal auditing in risk management and the incorporation of risk into the internal audit function's annual plan, relatively little information is available on the performance of a risk-based internal audit engagement. However, this does not mean that it is less

important. Studies (Deloitte & IIA (UK and Ireland) 2008; Ernst & Young 2008; PWC 2008(b); IIA Research Foundation 2009(a)) on the current and future trends in the internal audit profession all suggest that internal auditing will have to improve their risk-related competencies and mindset as well as be more effective and efficient in adding value to the organisation. One area where both these expectations can be adhered to is the performance of risk-based internal audit engagements.

4.4 INTERNAL AUDIT ASSURANCE ENGAGEMENTS

The definition of the profession describes internal auditing as a systematic and disciplined approach (IIA 2009(a):2). Thus, to perform an internal audit engagement requires a structured approach, regardless of the engagement type (financial, operational or compliance audit), the level of the auditee (strategic or operational, such as a business process or business unit) or the characteristics of the organisation (such as industry, country, size, culture). In this section the internal audit process, with specific reference to the planning phase and the engagement work programme, is briefly discussed as these are important elements of a risk-based internal audit assurance engagement.

4.4.1 Internal audit process

Lemon and Tatum (2003:270) and Reding *et al.* (2007:10-2) support the IIA's definition of an internal audit engagement being a systematic and disciplined process. This is consistent with the external audit profession's audit process based on the International Standards on Auditing (SAICA 2009/10:ISA200-2). For the internal audit profession, the *Standards* provide mandatory guidance on the performance of an internal audit engagement that includes four phases (IIA 2009(a):31-38). As these phases are compulsory and the structure is fixed, the four phases will only briefly be introduced. Thereafter the planning phase and the engagement work programme are discussed in more depth as they have a direct influence on this study.

- **Engagement planning**

This phase includes various planning considerations, engagement objectives, the engagement scope, resource allocation and finally setting an engagement work programme. The outcome of this phase is to develop an engagement work programme with detailed engagement procedures to be performed by the internal auditor.

- **Performing the engagement**

During this phase the engagement procedures, as determined by the previous phase, are executed. This phase includes the identification of relevant information, the analysis and evaluation of the information, documenting all activities and results, with all activities performed under appropriate supervision. The outcome is a list of findings substantiated by appropriate evidence.

- **Communicating results**

The findings, as determined in the previous phase, must be communicated to the appropriate parties. This phase includes communication criteria, the quality of the communication, the use of *Conducted in Conformance with the Standards* when an internal audit function has performed the engagement according to the *Standards*, and the distribution of the final communication.

- **Monitoring progress**

This is the final phase in the process. It is expected that the internal audit function should ensure that the requirements listed in the internal audit report are either implemented or that senior management has accepted the risk of not taking any actions. This phase thus entails a follow-up process to establish how recommendations have been treated.

4.4.2 Planning phase

According to *Standard* 2200 (IIA 2009(a):31) a plan must be developed and documented for each internal audit engagement that is performed. The external audit profession (SAICA 2009/10:ISA300-2) adds that the external audit engagement must be planned in such a manner that it is effective. The planning phase forms the basis of the rest of the engagement and is probably the most important phase. If the plan is unclear or not comprehensive enough, procedures will not be performed correctly or even excluded from the engagement. If, however, the plan is too comprehensive, valuable resources will be wasted, as the internal auditor will perform engagement procedures on areas where they are not needed. To perform an effective and efficient engagement thus entails that the planning phase must be carried out with the utmost care. In this section various considerations when planning an engagement are discussed. The evolution of the whole internal audit engagement and how it developed to include risk-based internal auditing is researched and debated later in the chapter.

According to *Standard* 2200 (IIA 2009(a):31-33) and related practice advisories (IIA 2009(a):121-129), the following aspects must be considered when planning an engagement:

- With regard to the activity under review, the following is line management's responsibility and the information is considered by the internal auditor during the planning phase:
    - all operations performed;
    - systems, records, personnel and physical properties used by the activity;
    - all resources allocated and used by the activity;
    - the activity's objectives and related criteria as well as how these are developed;
    - how performance is measured and managed against the objectives and criteria;
    - management assessment of risk, the process of monitoring, reporting and resolving risk and control aspects, the reporting and response of

events exceeding the risk appetite, and risk in other activities related to the activity under review;
    - significant risks threatening the activity as determined by line and senior management;
    - how the impacts of risks are kept within an acceptable level; and
    - the adequacy and effectiveness of risk management and control processes.
- The chief audit executive should establish an overall evaluation of the engagement in the context of the internal audit function by considering or performing the following:
    - determine whether the results are relied upon by others;
    - determine whether the engagement is related to current or potential litigations;
    - the complexity and scope of the engagement;
    - the value and future use of the outcome of the engagement as well as documents gathered and developed;
    - consider personnel matters including the size of the internal audit function, the experience level of internal auditors, and the use of internal staff members, guest internal auditors or external parties; and
    - determine engagement communication requirements.
- The internal audit function should perform the following duties:
    - obtain background information and evaluate the effect on the engagement – if needed, the function should conduct a survey to become familiar with the environment;
    - conduct a preliminary assessment of the risks threatening the activity (also consider management's assessment – refer to section 4.3.3.1.1 on p. 248);
    - consider the probability of errors, fraud, non-compliance and other exposures;
    - establish engagement objectives to address the risk areas;
    - if needed, develop appropriate evaluation criteria with management;
    - establish an engagement scope that will satisfy the engagement objectives;

- establish technical requirements and resource allocation based on the nature and complexity of the engagement, time constraints and available resources;
- develop an engagement work programme stating the nature and extent of testing to be performed; and
- develop ad hoc requirements such as the time frame and appropriate communication.

The above lists are mostly self-explanatory. An area that needs further debating is the inclusion of the concept of risk into the planning of the internal audit engagement. To determine what is required of the internal auditor in this regard, how he/she should go about performing these duties, and whether risk management methodologies can be used as a basis, the above IIA guidance is compared to the risk management process. In table 4.1 on p. 256, the risk-related elements with regard to the activity's responsibility (this could also be performed by a risk responsible body such as a risk department – refer to section 3.3.6.2 on p. 179) as well as the internal audit function's requirements are compared to the steps in the risk management process as discussed in section 3.5 on p. 191.

The comparison highlights a few facts that need further discussion. Firstly, it is important to note that the IIA recognises that without management and/or a risk department performing certain activities, the planning of an internal audit engagement is made extremely difficult. For example, if management has not determined the objectives and related criteria of the activity as a whole as well as the various operations within the activity, the internal auditor cannot determine the engagement objective and scope. He/she will first have to develop these elements in conjunction with line management. This is also applicable on all the other elements of the risk management process as highlighted in table 4.1 on p. 256. Secondly, when it comes to risk aspects, the IIA *Standards* expect internal auditors to plan their engagements based on the same elements as the risk management process performed by management and/or the risk department. This implies that if the risk management process is well performed and properly documented (such as a risk register), the internal auditor could use the outcome

of the internal risk management process as the starting point for the planning of the audit engagement.

Table 4.1: The IIA internal audit engagement planning linked to the risk management process

Step in risk management process	Management/Risk department's responsibility (refer to above list)	Internal audit planning considerations (refer to above list)
Objective setting	• Objectives and criteria developed	• Consider activity's objectives and criteria • Develop if no activity criteria exist • Develop engagement objectives and scope to address risk areas
Identification of risks	• Significant risks identified • Risk in related areas (holistic)	• Consider all relevant exposures
Assessment of risks	• Assessment of risks • Monitor, report and resolve risk aspects • Impact of risk within acceptable level (risk appetite) • Report on risks exceeding risk appetite	• Consider management's assessment and use if reliable • If none or not reliable, conduct own survey and assessment
Risk responses	• Response on risk exceeding risk appetite • How impact is kept within acceptable risk level	• Consider management's report and response on risks exceeding risk appetite (potential critical control aspects)
Risk communication and monitoring	• Adequate and effective process	• Consider management's processes on report and monitor risk aspects

Figure 4.2 on p. 257 summarises the above, distinguishing between what is the responsibility of management and/or the risk department and the internal audit function, as well as how these two can compliment one another.

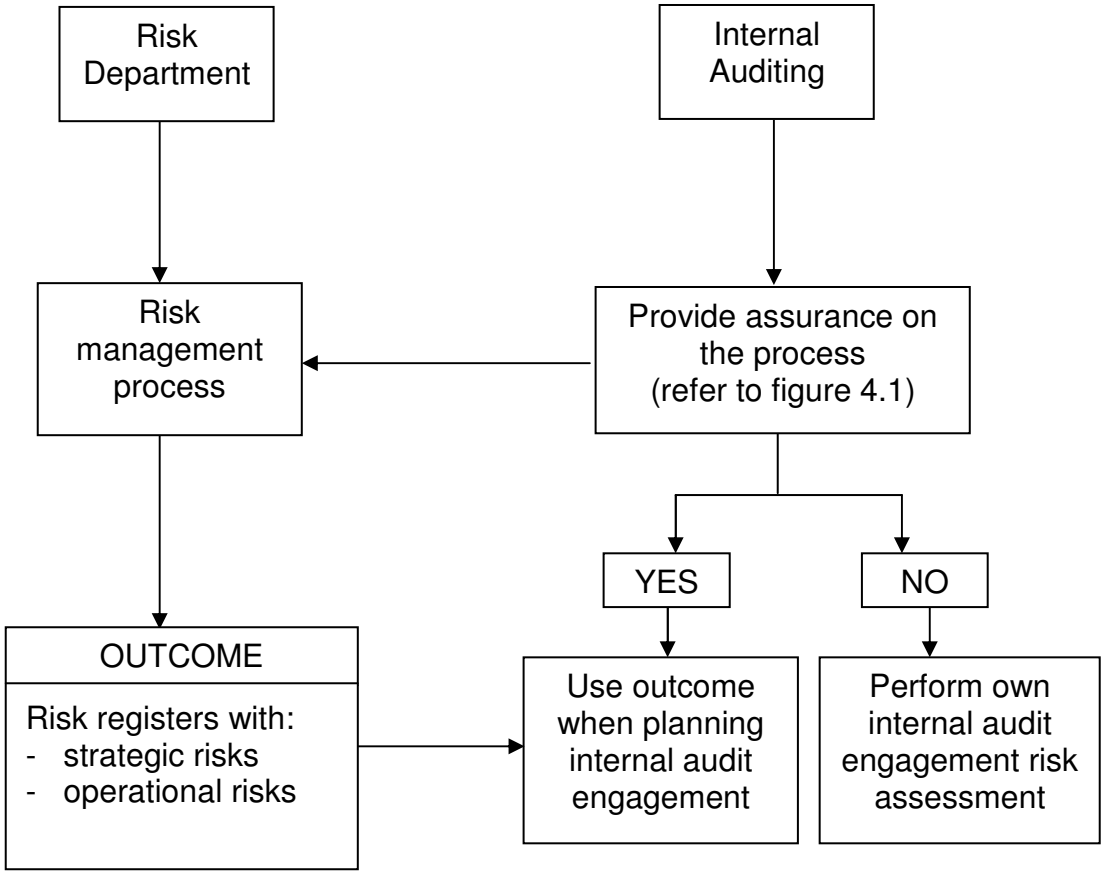


Figure 4.2: The risk management process and internal audit engagement planning

4.4.3 Engagement work programme

The outcome of the engagement planning is the engagement work programme that consists of a list of engagement procedures that must be performed by the internal audit team to gather evidence that management's criteria are being met – thus achieving the engagement's objectives (Lemon & Tatum 2003:282). As mentioned in the previous section, the planning phase is probably the most important step in the whole process. The engagement work programme is the final product of this phase and the procedures it lists will guide the internal auditor while identifying, analysing, evaluating and documenting information (IIA 2009(a):33). If this list is thus not complete, or is too vague or too comprehensive, it will have an effect on the procedures performed, evidence gathered and ultimately on the results of the engagement.

A list of engagement procedures that is too comprehensive could result in engagement procedures being performed unnecessarily, thus wasting the internal auditor's time and other resources. Although the *Standards* do not mention that the internal audit engagement must be performed effectively and efficiently, it is mentioned (IIA 2009(a):26) that the internal audit function's resources must be deployed in an appropriate (knowledge, skills and competencies needed), sufficient (quantity) and effective (optimise the achievement of the internal audit annual plan) manner. With the threat of a possible scarcity of competent and skilled internal auditors (refer to section 2.6.3 on p. 119), this could mean that internal audit engagements should be planned in such a manner that fewer more efficient engagement procedures should be performed to achieve the engagement's objectives.

4.4.4 Conclusion

Although the internal audit assurance engagement process consists of four phases, it is clear that the planning phase, being the foundation of the rest of the process, is a very important element. The outcome of this step, namely an engagement work programme, will guide the internal auditor on what must be done, how it must be done, when and by whom. With the possible future shortage of competent internal auditors, it is important to deploy the internal audit function's resources optimally. The IIA *Standards* recognises that the outcome of the risk management process (if reliable) can be used in the planning phase of the internal audit engagement, ultimately ensuring a more effective and efficient process. This is also referred to as performing a risk-based internal audit engagement.

4.5 RISK-BASED INTERNAL AUDIT ENGAGEMENT

There are many examples in the literature (McNamee & Selim 1998:199; Spencer Pickett 2003:12; Griffiths 2006(b):43; IOD 2009:94) that refer to risk-based internal auditing, mainly reflecting on the role that internal auditing should play with regard to the risk management framework and/or process. Some of the literature (Rivenback 2000:19; Spencer Pickett 2003:518; Wheeler 2005:15-16;

Lubbe & Van der Merwe 2007:25; Pelletier 2008:73; Koutoupis & Tsamis 2009:106; IOD 2009:94) also refers to the internal audit function's annual plan based on the strategic risks when using the term risk-based internal auditing. Both these scenarios ignore the potential to use risk strategies as the basis for internal audit engagements. Furthermore, a study performed amongst Greek banks' internal audit methodologies (Koutoupis & Tsamis 2009:102) revealed that many internal audit functions, although using the term risk-based internal auditing, could not prove it by providing any form of a risk assessment or risk-based audit plan, undermining the term risk-based internal auditing even further.

In the rest of this section, the term risk-based internal auditing is debated, with specific reference to an assurance engagement. The evolution of internal audit engagements and the current trend is discussed, where after some of the most important elements that are needed for a risk-based internal audit engagement to be successful are investigated. Lastly, various risk-based internal audit models are compared to assist in the development of a preliminary model.

4.5.1 Introduction to a risk-based internal audit engagement

As discussed in sections 1.2 on p. 4, 1.3 on p. 12 and 2.2 on p. 58, internal auditing has been influenced over the last few decades by the changing business environment, and has undergone, and still is undergoing a number of transformations. Internal auditing, true to its current definition (refer to section 2.4.1 on p. 70), has evolved from focusing on controls and reporting to management on the control activities performed by employees, to fully fledged business advisors focusing on aspects of risk management, control and corporate governance. Ultimately, these changes have had and are still having an effect on the way internal audit activities are being performed, including the internal audit assurance engagement process. Table 4.2 on p. 260 briefly explains this change and how it has affected the internal audit engagement process with specific reference to risks and controls. The word risk is only mentioned from the second generation, referring to financial and compliance risk only. It is only from the 1990s and onwards that risk is more broadly incorporated into the engagement process.

Table 4.2: Evolution of the internal audit engagement

Engagement elements	1st Generation (pre 1980)	2nd Generation (1980s)	3rd Generation (1990s)	4th Generation (2000+)
Audit response	Re-active (after the action/ activity occurred)	Re-active (after the action/ activity occurred)	Pro-active (identify potential problems)	Co-active (real-time and part of strategic plan)
Assurance service	Control-based	Control frame-work-based	Business risk-based	Risk manage-ment process-based
Starting point of engagement	Existing processes, procedures and control activities	Financial and compliance risks	Thorough under-standing of the business and various business risks	Thorough under-standing of the business and various business risks
Additional steps and/or information during planning	None	Determine controls that should be in place	Determine controls that should be in place	Determine the risk management process(es) that should be in place to effect-tively manage key risks
Engagement procedures	Audit for: • compliance	Audit for: • effective control design • operational effectiveness • compliance	Audit for: • effective control design • operational effectiveness • compliance	Audit within each risk management process component for: • effective control design • operational effectiveness • compliance
Testing	Use sampling techniques ignoring risks	Use sampling techniques including financial and compliance risks	Use sampling techniques including all business risks	Continuous testing and focus on high risks (target testing)

(Source: Hyde 2007:65-68; Hollyman 2006:6; Spira & Page 2003:653-656; McNamee & Selim 1998:5)

This change with regard to the incorporation of risk into the internal audit engagement process can be contributed to the increased interest in, and implementation of risk management in the business environment. Internal auditors should assist management in mitigating the key risks and thus delivering value at the highest levels of their organisation. Therefore, when performing individual internal audit engagements, the focus should be on the risks threatening the operational objectives of the activity under review, addressing the high-risk areas and performing few or even no audit procedures on the low-risk areas.

Studies (IIA Research Foundation 2007:216-233; Ernst & Young 2008:59; Deloitte 2008:13-14; PWC 2008(a):16-19; PWC 2008(b):31-35; IIA Research Foundation 2009(a):9) on the current and future trends of the internal audit profession support the movement to auditing more effectively and efficiently. Topics such as risk-based internal audit engagement planning and continuous internal auditing are mentioned as the basis for modern internal audit methodologies. However, whether all the studies evaluate the concept of risk-based internal auditing using the same principles is debatable. Although many agree that internal auditing has to adapt to the changing landscape, including the use of more streamlined internal audit tools and techniques, it is not clear whether using risk-based internal audit methodologies when performing an internal audit engagement is viewed on the same basis.

4.5.2 The definition of risk-based internal audit engagements

Being that risk-based internal auditing is a fairly new methodology for the internal audit profession, not much literature is available on the topic. This fact is supported by Koutoupis and Tsamis (2009:104) who confirm that the literature review on this topic includes mostly discussions on risk management and the role internal auditing should play, as well as the internal audit risk assessment process and the effect on the internal audit annual plan. The few relevant definitions remaining, after the literature covering the above two areas is eliminated, are discussed below:

Internal auditing provides an independent and objective opinion to an organisation's management as to whether its risks are being managed to acceptable levels (Griffiths 2006(a):26).

…risk-based internal auditing is to provide assurance on those risk management processes which cover all significant risks threatening the objectives of the organisation…elements which the head of internal audit needs to consider:

- The extent to which the board and management determine, assess, manage and monitor risks…
- The existence of a risk register… and the extent to which this may be relied upon for audit planning.
- The compilation of an audit universe…
- The conduct of individual audits, which conclude on whether inherent risks above the risk appetite are being controlled to reduce them to within the risk appetite (Griffiths 2006(b):9).

Risk-based audit (planning) is about targeting high-risk areas for audit coverage; promoting a discussion of risk with management; starting with risk as the first step in the risk-based auditing process… (Spencer Pickett 2006:205).

The objective of risk-based internal auditing is to provide independent assurance to the board that:

- The risk management processes…within the organisation (covering all risk management processes at corporate, divisional, business unit, business process level, etc.) are operating as intended.
- These risk management processes are of sound design.
- The responses which management has made to risks which they wish to treat are both adequate and effective in reducing those risks to a level acceptable to the board.

- …a sound framework of controls is in place to sufficiently mitigate those risks which management wishes to treat (IIA (UK and Ireland) 2003:1).

Audits that focus on risk… (McNamee & Selim 1998:199).

From the above definitions a few characteristics of a risk-based internal audit engagement can be derived. Firstly, risk-based internal audit engagements are based on a sound risk management process:

- implemented by management;
- covering all levels within the organisation; and
- with an output listing all applicable risks (risk register).

Secondly, when performing a risk-based internal audit engagement, the internal auditor should ensure that the engagement process:

- treats risk as the main element instead of other elements such as controls;
- focuses on high-risk areas;
- investigates whether risks are within acceptable levels; and if not
- evaluates the adequacy and effectiveness of management's responses to mitigate the risks to acceptable levels, including controls.

The above summary is consistent with the findings in table 4.1 on p. 256 and figure 4.2 on p. 257 where the IIA's guidance on the planning of an internal audit engagement is compared with the risk management process. It would be extremely difficult and even impossible to implement an effective risk-based methodology for an internal audit engagement without having a proper risk management process in place that has been performed by management (reflecting the organisation's risk maturity). A second prerequisite is that the outcome of the risk management process, or at minimum the risk assessment, must be documented (in a risk register). Lastly, the assessment should be

performed on all possible levels including strategic, business units, and business processes and/or systems (reflecting on a holistic risk management process).

4.5.3 Elements needed to perform a risk-based internal audit engagement

In the previous section it is concluded that the steps in the risk management process can be used by the internal audit function to perform internal audit engagements using a risk-based approach. However, for a risk-based internal audit engagement to be successful, certain elements must be present in the organisation. The three main elements are the risk maturity of the organisation, a risk register(s) documenting all the necessary risk-related information, and lastly, the performance of risk assessments for specific processes, systems, business units, etc., also referred to as operational risk assessments.

4.5.3.1 Risk maturity

As discussed in section 3.6 on p. 205, the risk maturity of an organisation is determined by the extent to which a risk management strategy has been adopted and applied, as planned, by management (De la Rosa 2008(b)). The more relevant activities and elements of the risk management framework management have implemented effectively, the more risk mature the organisation is. According to bodies such as the IIA (UK and Ireland) (2003) and IIA (2009(e):par 8), as well as individuals providing guidance on risk-based internal audit engagements (Griffiths 2006(a):23; Griffiths 2006(b):15-17; De la Rosa 2008(b); Baker 2010:32), the risk maturity of a specific organisation will have an enormous effect on how risk concepts can be incorporated into an internal audit engagement. The fist step, before deciding whether or not to use a risk-based internal audit approach, should be to determine the risk maturity of the organisation as a whole and for the specific activity under review (refer to section 4.5.3.3 on p. 267 for a discussion on holistic *versus* silo risk management). Table 4.3 on p. 265 summarises the possible effect of the risk maturity of an organisation on the internal audit engagement and what the internal auditor's approach should be in different scenarios. In the first column the risk maturity terminology is provided

with an explanation of the characteristics associated with each level explained in the second column.

Table 4.3: The effect of risk maturity on a risk-based internal audit engagement

Risk maturity level	Characteristics	Internal audit approach	Effect on risk-based internal audit engagement (RBIA)
Naïve	• No formal risk management approach	• Promote risk management • Provide consultation for risk management framework	• RBIA not possible • Perform risk-driven audits (own risk assessment)
Aware	• Scattered silo risk management approach	• Promote enterprise-wide risk management approach • Provide consultation for risk management framework	• For specific activity under review (if available): o audit risk assessment • Perform RBIA (limited)
Defined	• Risk management strategies in place	• Facilitate current risk management • Liaise with risk management structures • Use assessment where possible (quality may vary)	• For specific activity under review: o review risk maturity o audit quality of risk assessment • If poor, no or limited RBIA • If acceptable, perform RBIA
Managed	• Enterprise-wide risk management approach	• Audit risk management processes	• Use risk assessment output to perform RBIA • If necessary, consult on risk responses
Enabled	• Risk management fully embedded	• Audit risk management processes	• Use risk assessment output to perform RBIA

(Source: IIA (UK and Ireland) 2003; Griffiths 2006(b):15-17; De la Rosa 2008(b))

It should be noted that although the terms ‘managed’ and ‘enabled’ seem to differ only slightly, the difference nevertheless significantly affects the duties internal auditing will perform. ‘Managed’ refers to the whole risk management process performed on a holistic basis, but the risk management framework could still lack some guidance. For internal auditing, although the internal auditor can rely on the risk assessment performed by management, the implementation of the risk

responses most probably still needs close attention. 'Enabled' refers to both the risk management framework and risk management process being fully incorporated into the strategic and daily activities of the organisation (refer to section 3.3.1 on p. 153).

The effect of risk maturity on the performance of an internal audit engagement is explained by means of an example. Where an organisation is risk naïve, thus having developed no or little formal approach to risk management, the risk management process will either be non-existing or of a poor standard. For a specific activity, risks will not have been identified, assessed and managed according to a structured approach. To perform a risk-based internal audit engagement, the internal auditor will have to perform his/her own risk assessment. This could be a lengthy process and not cost-effective for the internal audit function. If, however, the organisation is risk managed or risk enabled (IIA (UK and Ireland) 2003), where there is an enterprise-wide approach to risk management, the internal audit function should audit the risk management process (refer to section 4.3.1 on p. 234), where after the output of the operational risk assessment for the activity under review can be used in the risk-based internal audit engagement as appropriate.

4.5.3.2 Risk register

As discussed in section 3.5.3 on p. 203, a risk register is a document which keeps track of the outcome of the risk management process of various organisational activities on different levels (strategic and operational). The level of risk maturity of the organisation will determine whether the organisation has a comprehensive risk register or not. Thus, the more risk mature the organisation is, the more likely that a proper risk register is kept (Griffiths 2006(b):16). Therefore, when the internal auditor can rely on the risk management process, the outcome of the process that is documented in the risk register should be used to determine the priorities of the risk-based internal audit engagement.

The risk register, also known as a risk database (Spencer Pickett 2006:81) consists of detailed information on risks identified, assessed and managed by

different management levels. Internal auditing should use this information to guide them (McNamee & Selim 1998:5-6; Spencer Pickett 2003:139-141; Griffiths 2006(b):18,28; Spencer Pickett 2006:84-85; Lubbe & Van der Merwe 2007:26), firstly to determine the audit universe as part of the internal audit function's annual planning (usually the strategic risks of the organisation), as well as in the planning of an internal audit engagement (usually the operational risks for a business process and/or unit).

With reference to the planning of an internal audit assurance engagement, the risk register, containing all the risks identified, assessed and managed by the line managers responsible for the specific activity under review, should form the basis of a risk-based approach. It is therefore appropriate to conclude that if:

- an organisation is risk mature;
- it would have a structured and well-developed risk management process in place;
- on which the internal audit function would be able to rely and;
- use the outcome of the process (risk being identified and assessed);
- that is documented in a comprehensive risk database (register);
- to guide the planning phase of the internal audit engagement.

4.5.3.3 Operational risk assessment

With the above conclusion, it seems that for a risk mature organisation, a risk-based internal audit approach is the most efficient way to manage internal audit resources. However, it could be possible that even in a risk mature organisation only strategic risks are determined by using a risk management process (Shenker & Walker 2006:33; Hespenheide, Pundman & Corcoran 2007:6; Griggs 2008:45; Killackey 2009:29) and that risk related to specific business units or processes are either not managed or managed within a silo (refer to section 3.7.1.2 on p. 217). The danger of this approach is firstly that strategic objectives, being dependent on the achievement of operational objectives, will not be fully reached. Secondly, when business units or processes manage risks within a silo, it is

possible that certain risks are not properly addressed. For example, the human resources department has determined the risks threatening the appointment of new employees and is managing these risks. The financial department has determined the risks regarding the payment of fictitious employees and is managing these risks. However, these two departments have not communicated with one another regarding these risks and it may perhaps be possible that a fictitious employee can be appointed and paid. Examples of where the lack of managing operational risks has led to fraud and other malpractices (Martin 2009/10:78-82) include Barings Bank, Citigroup, Societe Generale, Northern Rock, HBOS, USB and AIG, to name but a few.

When performing a risk-based internal audit approach for an assurance engagement, it is thus a prerequisite that risks have been identified, assessed and managed for the activity under review, whether it is a strategic-based engagement (to a lesser extent) or an operational-based engagement. For a risk mature organisation, if the risks have been identified and assessed by the appropriate managers, internal auditing can rely on the outcome and base the engagement planning on the information gathered from the risk register.

4.5.4 Risk-based internal audit engagement models

In table 4.2 on p. 260 the evolution of the internal audit engagement is sketched. Although the word risk is mentioned in the second generation methodology, it is only from the third generation onwards that risk is a more prominent factor in the performance of an internal audit engagement. Risk is extensively mentioned in both the third and fourth generation methodology internal audit engagement models. However, the question remains as to which of these two methodologies are used when referring to risk-based internal audit engagements.

4.5.4.1 Basis of risk-based internal audit models

In table 3.4 on p. 193, various risk management process models are compared. One of the most comprehensive models is the COSO Report (2004). At first glance it seems that this model is the basis for the fourth generation internal audit engagement process. The first COSO Report (1992) focuses on controls that can

mitigate risks identified. It could thus be possible that this model reflects on the third generation internal audit engagements. Therefore, in table 4.4 below, the third and the fourth generation internal audit engagements planning elements (refer to table 4.2 on p. 260 which analyses the evolution of the internal audit engagement) are connected to the COSO reports (1992, 2004). These two documents are briefly mentioned in section 2.5.2.2 on p. 92 and the second COSO model is further discussed in section 3.5 on p. 191 with regard to the risk management process.

Table 4.4: Comparing evolution of internal audit engagements with the COSO models

Engagement planning elements	COSO I	COSO II
Starting point	Based on the **risk assessment** of all business activities; understand all risks	Based on the outcome of the **risk management process**; understand all risks
Additional steps and/or information during planning	Determine **controls** that should be in place to **mitigate the risks**	Determine the **risk response** that should be in place to effectively **manage key risks**
Engagement procedures	Not specific scope – determined by previous element	Audit the management of key risks within each risk management process component
Scope	**All** business risks	**Target** testing focusing on high risks

Based on this comparison, it could be concluded that the third generation risk-based internal audit engagement is based on the first COSO model (1992) or similar models, whereas the fourth generation is based on the second COSO model (2004) or similar models.

In the rest of this section, the two COSO models (1992, 2004) are used to identify the elements and criteria used in a risk-based internal audit engagement. Furthermore, whether risk-based internal audit engagements currently performed are based on a control-centric (COSO I) or risk-centric (COSO II) approach, is investigated.

4.5.4.2 Comparison of different internal audit methodologies

Although it seems that in modern internal auditing the term risk-based internal auditing is widely used, what it is used to describe is not consistent. As mentioned in section 4.5 on p. 258, the literature refers to the audit of the risk management process or the annual plan of the internal audit function based on risk. When it comes to performing risk-based internal audit engagements, various methodologies are debated by researchers and are being used by different organisations. In table 4.5 on p. 272 some of the most prominent methodologies in the literature are compared by using the steps of the two COSO models, thus referring to the third and fourth generation internal audit engagements. The comparison only focuses on elements relevant to the planning of an internal audit engagement, specifically referring to the establishment of the engagement work programme with its detailed engagement procedures.

The table is divided between the first and the second COSO models. For each model, the two columns named 'step' refer to the steps in the particular COSO model as discussed in the COSO reports (1992, 2004). For the sake of a meaningful comparison, when a specific step is not mentioned in the COSO report, it is indicated as 'N/A' or not applicable. The second and fifth columns explain the elements present within each step. The third and the last columns have two functions. They first list the literature sources that indicate that these models are used when referring to risk-based internal audit engagements, and secondly, the weaknesses identified when comparing the elements in column two and five with the literature.

The first conclusion reached from this comparison and analysis is that it seems that not much literature is available on the topic. After a thorough search of the Internet and various research databases, only a few studies were found. Secondly, with reference to table 4.4 on p. 269, the fourth generation refers to the second COSO model (2004). However, the internal audit engagement process used in much of the literature still refers to the first COSO model (1992) as reflected in the literature sources and their respective dates that are linked to the first COSO model (Spencer Pickett 2003; Deloitte 2005; Spencer Pickett 2006;

Sobel 2008; Clayton 2009). Thirdly, it seems that although these two models are mainly used, there are still areas that are not incorporated into the internal audit engagement process. When referring to the second COSO model and the fourth generation internal audit engagement process (column 6 in table 4.5 on p. 272), five areas that could still be developed include the following:

- The internal auditors perform their own risk assessment based on the activity's objectives. If the formal risk management process's risk assessment is used, valuable time could be saved. However, this will only be possible if the organisation is risk mature (refer to section 4.5.3.1 on p. 264) and the risk management process has been audited by the internal audit function and is found to be reliable (refer to section 4.3.1 on p. 234).
- Previously, 'risk' referred mainly to hazards. The modern approach to risk includes the loss of opportunity as a risk (refer to section 3.4.3.3 on p. 189). It seems that this concept is still not incorporated into the fourth generation internal audit engagement planning.
- According to the risk management process, the difference between the inherent risk and the residual risk is the current responses in place to mitigate the risk to an acceptable level (refer to section 3.4.4 on p. 189). The movement between these two levels should thus provide the internal auditors with a starting point when planning the engagement procedures. However, it seems that this is not currently the case.
- As mentioned before (refer to section 3.7.1.2 on p. 217), risk cannot be viewed in silos but has to be viewed holistically. With reference to an internal audit engagement, this could mean that a risk identified in a specific business unit or process might flow over to another. The internal auditor should review the effect of these risks on the whole instead of the smaller unit.
- It seems that controls are mostly investigated as a means of the risk response of reducing risks. Other mitigating procedures as well as risk response categories (refer to section 3.5.2.4 on p. 201) are not mentioned, but could be more favourable to use, for example, be more cost effective.

Table 4.5: COSO I and COSO II used in practice as part of the internal audit engagement planning process

COSO I			COSO II		
Step	**Applicable detail elements**	**Use in internal audit engagement (Sources)**	**Step**	**Applicable detail elements**	**Use in internal audit engagement (Sources)**
N/A		Literature sources: • McNamee & Selim 1998 • Bank of Canada 1998 • Spencer Pickett 2003 • Deloitte 2005 • Spencer Pickett 2006 • Sobel 2008 • Clayton 2009 All elements used except (weaknesses): • Risk analysis not used (McNamee & Selim 1998:103-105; Spencer Pickett 2003:402; Clayton 2009:35-39) • Test only controls that mitigate risks (McNamee & Selim 1998:106; Deloitte 2005:7) • No integration of controls and risk	Objective setting	• Strategic objectives • Related objectives including operations objectives • Risk appetite and tolerance	Literature sources: • Reding *et al.* 2007 • Griffiths 2006(a) • Griffiths 2006(b) • Pelletier 2008 All elements used except (weaknesses): • Perform own risk identification and risk assessment only (Reding *et al.* 2007:10/23-10/30; Pelletier 2008:73-76) • No mentioning of opportunity risks (Griffiths 2006(a):41-42; Reding *et al.* 2007:10/23-25; Pelletier 2008:73-76) • Do not incorporate difference between inherent and residual risks into plan (Griffiths 2006(b):37-40; Reding *et al.*
N/A			Event identification	• Events including risk categories • Risks and opportunities for each category	

Risk assessment	• Objective setting
	• Risk identification
	• Risk analysis:
	  ○ significance
	  ○ likelihood
			Risk assessment	• Inherent and residual risks
				• Risk analysis:
				  ○ likelihood
				  ○ impact
				• Holistic view of risk, e.g., affecting multiple business units or processes	

N/A			Risk	• Evaluate possibilities	

COSO I			COSO II		
Step	**Applicable detail elements**	**Use in internal audit engagement (Sources)**	**Step**	**Applicable detail elements**	**Use in internal audit engagement (Sources)**
		assessment (Spencer Pickett 2003; Sobel 2008:93) • Perform own risk assessment including evaluating management's efforts (Spencer Pickett 2006:143-161; Sobel 2008:93) • Assess all elements individually and link values which prioritise audit effort (Bank of Canada 1998:9-11) • Only financial assertion based (Deloitte 2005:1-10)	response	with regard to: ○ effect on likelihood and impact ○ cost *versus* benefit ○ new opportunities • Selected types: ○ avoid (eliminate activity that causes risk) ○ reduce (various actions including controls) ○ share (transfer or share risk) ○ accept (risk within acceptable level)	2007:10/34-10/36; Pelletier 2008:73-76) • No holistic view (Griffiths 2006(a):30; Reding *et al.* 2007:10/25-10/26; Pelletier 2008:73-76) • Link only controls as risk response to risk assessment (Griffiths 2006(a):42; Reding *et al*. 2007:10/30-10/34; Pelletier 2008:73-76)
Control activities	• Integrate with risk assessment		Control activities	• Integrate with risk response	

(Source: refer to discussion)

It seems that although some individuals and organisations are promoting the performance of risk-based internal audit engagements based on the risk management process, and more specifically the model in the second COSO Report (2004), there are still a few gaps that prevent the utilisation of the process to its fullest potential.

4.5.5 Preliminary risk-based internal audit engagement model

While reflecting on the above gaps as well as the IIA's internal audit engagement planning requirements based on risk as given in table 4.1 on p. 256, in this section it is debated whether a risk-based internal audit engagement model can be developed using the risk management process as discussed in section 3.5 on p. 191. In table 4.6 on p. 275 the steps in the risk management process directly linked to the planning phase of an engagement are used as the starting point in the development of a preliminary risk-based internal audit engagement model. This model is based on the following assumptions:

- The organisation is risk mature and thus has a comprehensive risk management process (for both strategic and operational levels) in place. It is being driven by the board and senior management and implemented by a body independent from the internal audit function, such as a risk department (refer to sections 4.5.3.1 on p.264 and 4.5.3.3 on p. 267).
- The risk management process and its outcome are properly documented, for example in a risk register (refer to section 4.5.3.2 on p. 266).
- The risk appetite and risk tolerance levels have been set by senior management and the board, or where applicable by line-management for operational activities (refer to sections 3.5.2.3.1 on p. 200 and 3.5.2.3.2 on p. 200).
- The risk management process has been audited by the internal audit function and the outcome of the process can be relied upon (refer to section 4.3.1 on p. 234).

Table 4.6: Incorporating the risk management process into the internal audit engagement process

Step	Risk management process (performed by management, e.g. risk department)	Use in internal audit engagement planning (for a specific activity under review e.g. business unit or business process)
1	• Objective setting (refer to section 3.5.2.1 on p. 195) • Outcome (a list of): o strategic objectives o operational objectives	• The activity's objectives and related criteria form the foundation of the audit engagement objectives and scope: o Review the objective setting process and outcome and, if needed, identify further objectives or only focus on priority objectives (based on the audit resources available) o Set the engagement objectives and scope
2	• Identification of risks (refer to section 3.5.2.2 on p. 196) • Outcome (a list of significant): o hazards o opportunities that threaten the reach of objectives	• The risks threatening the activity's objectives form the foundation of the engagement planning: o Consider the risk identification process and all relevant exposures identified according to the process o While obtaining knowledge of the activity, consider other exposures and risks for both hazards and opportunities threatening the reach of the activity's objectives
3	• Assessment of risks (refer to section 3.5.2.3 on p. 198) • Outcome (for each risk the measure of): o likelihood o impact o inherent risk-level o residual risk-level	• The assessment (likelihood and impact) of both the inherent and residual risks are determined: o Consider the risk assessment process and use outcome or perform own assessment o Review inherent risk level, current risk responses in place, and residual risk level for each risk o Measure inherent and residual risk level in the context of the risk appetite o Focus more on high level risks (inherent risk exceeding the risk appetite) o For the engagement programme, include current existing responses where the inherent risk is high but the residual risk is within the risk appetite levels o Investigate whether these responses are functioning as planned o Consider low inherent risk for inclusion in the

Step	Risk management process (performed by management, e.g. risk department)	Use in internal audit engagement planning (for a specific activity under review e.g. business unit or business process)
		engagement programme by using professional judgement ○ Consider high inherent risk where the residual risk remains high for inclusion in the engagement programme by using professional judgement
4	• Risk response (refer to section 3.5.2.4 on p. 201) • Outcome (for each risk decide to): ○ avoid ○ reduce ○ share ○ accept ○ exploit ○ terminate activity ○ integrate above	• The assessment of each risk is measured in terms of the risk appetite • Residual risk exceeding the risk appetite must be further treated by means of an appropriate risk response: ○ Consider engagement recommendation in terms of the appropriate risk response ○ Include in the follow-up phase of the engagement

The above identifies how the steps in the risk management process can be incorporated when performing an internal audit engagement. The use of the risk management process as the basis for a risk-based internal audit engagement can be explained by means of a schematic presentation as reflected in figures 4.3 on p. 277 and 4.4 on p. 279.

In figure 4.3 on p. 277, the steps in table 4.6 on p. 275 are explained as follows:

- Step 1 and 2 – Inherent as well as residual risks threatening the objectives are identified (reflected as number 1 where light blue reflects inherent risk, dark blue reflects residual risk, and the arrow reflects the current controls in place to mitigate the risk).
- Step 3 – The risks are assessed (measured) according to their likelihood of occurrence and/or impact on the organisation (reflected by where they are on the matrix).

- Step 4 – The risk responses are determined by the assessment of the residual risk.

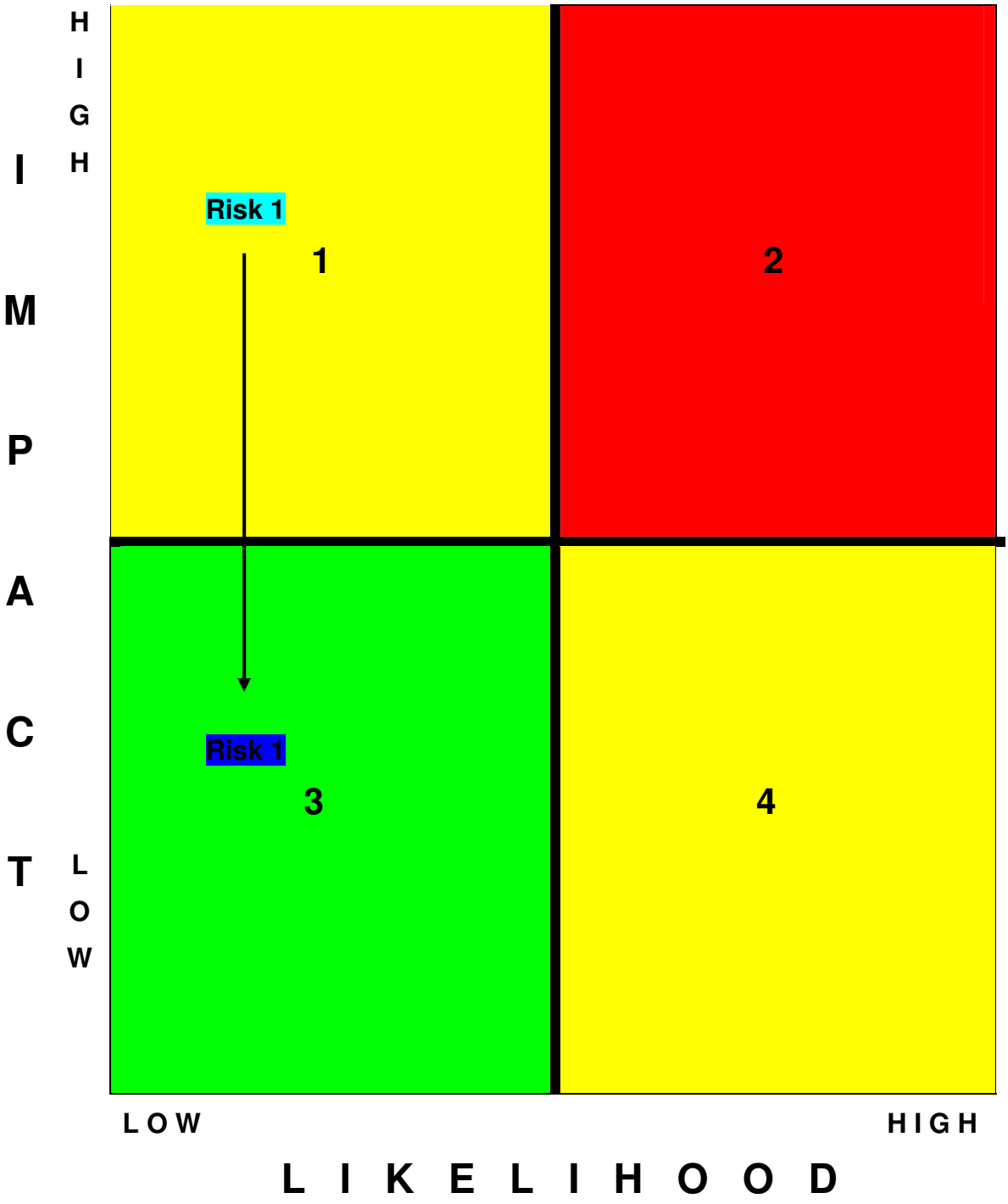


Figure 4.3: Mitigation of risks according to the risk management process

Further explanation of figure 4.3 above, linked to the risk management process, entails the following:

- The black cross in the middle of the figure refers to the risk appetite that management is prepared to accept.
- The vertical (impact) and horizontal (likelihood) axes are linked to the risk assessment measurement levels (refer to section 3.5.2.3 on p. 198).
- The only risks acceptable to management are the risks in the green section (quadrant 3). Inherent risks in this quadrant do not have to be mitigated as they are already within an acceptable level.
- Risks in the red section (quadrant 2) are the risks that can result in huge losses or even the closure of the organisation. These risks must be avoided by eliminating the activity, or if this is not possible, the risks must be managed carefully and monitored regularly.
- Risks in the yellow sections (quadrant 1 and 4) are the risks that should be managed. Risks with a high likelihood of occurrence (quadrant 4) should be managed by mainly implementing controls, and risks with a significant impact (should they occur) (quadrant 1) should be managed by sharing the risk.
- The aim of management is to mitigate the inherent risks in quadrants 1, 2 and 4 in such a manner that the residual level of these risks will be reflected in quadrant 3, thus within the acceptable level of risk taking.

In figure 4.4 on p. 279 and in the subsequent explanation of each risk, the use of the mitigation of risks according to the risk management process (refer to table 4.6 on p. 275, figure 4.3 on p. 277 and the related explanations) is linked to the performance of a risk-based internal audit engagement. Each risk is evaluated by the internal auditor with regard to the inherent risk level, the residual risk level and the risk appetite, to determine how and/or whether it should be included in the internal audit engagement programme. For each risk, the highest figure is the inherent risk level, the arrow is the current procedure(s) in place to mitigate the risk, and the lower figure is the residual risk or remaining risk after steps have been taken to lower the risk.

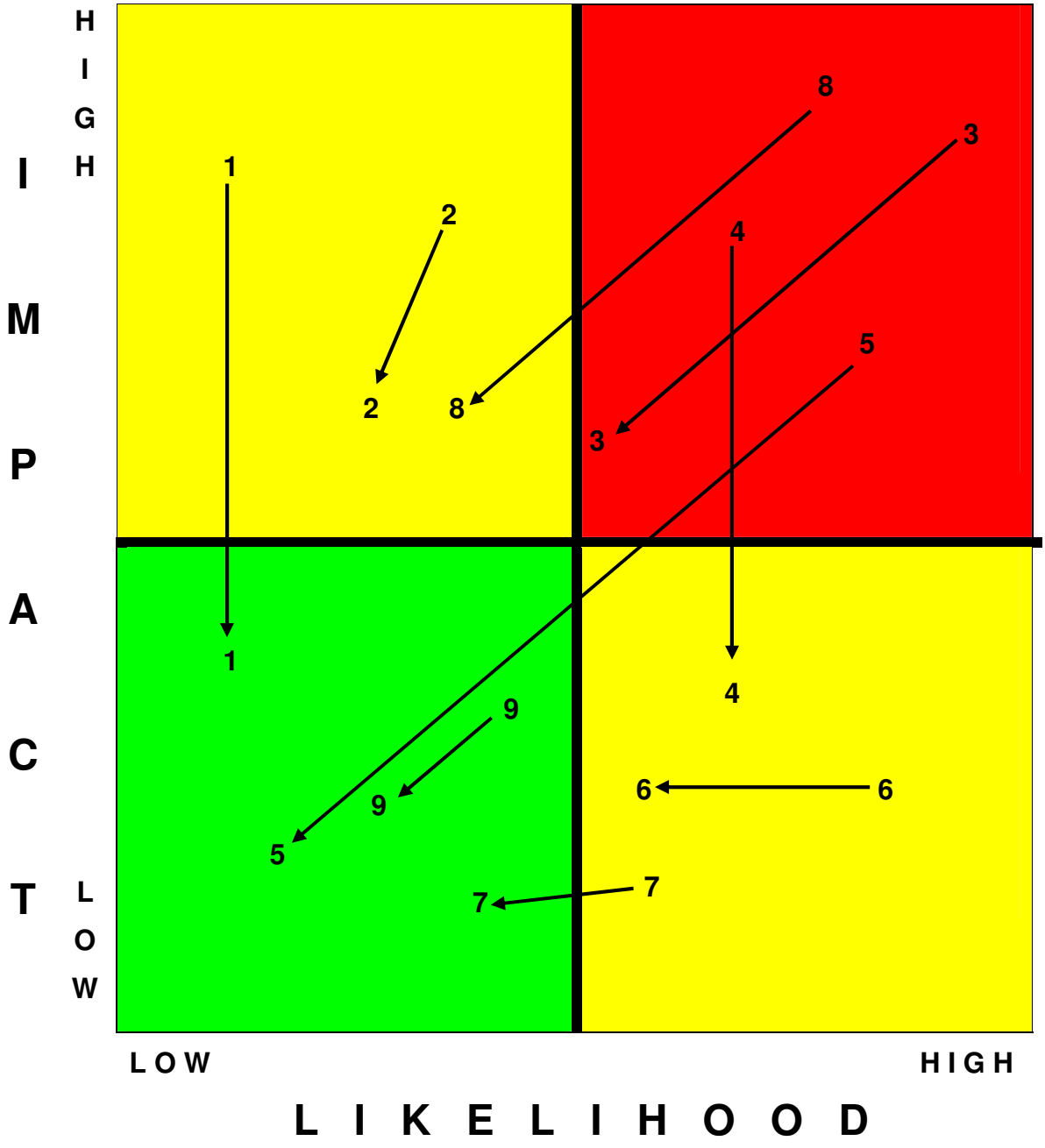


Figure 4.4: Risk-based internal audit engagement based on the risk management process

- Risk number 1 – The inherent risk is reduced by, for example, taking out insurance and the residual risk is therefore within the risk appetite. The auditor should include the inspection of the controls and other activities that mitigate the risk in the engagement work programme for:
  - the efficiency and effectiveness to mitigate the risk; and

- if these are acceptable as risk mitigation procedure(s), then the finding is one of compliance.

- Risk number 2 – Although the impact for the residual risk has decreased slightly, it is still not within acceptable risk levels. The internal auditor should report to management and recommend further mitigation procedures. Only those controls that mitigate the risk effectively and efficiently should be included in the engagement work programme. The auditor should recommend the elimination of inadequate controls that do not contribute to the mitigation of the risk.
- Risk number 3 – The residual risk is still not within acceptable risk levels. This should be reported as a matter of urgency to management and further mitigation procedures or the elimination of the activity should be recommended. The auditor should include only those controls in the engagement work programme that mitigate the risk effectively and efficiently; he/she should recommend the elimination of inadequate controls that do not contribute to the mitigation of the risk.
- Risk number 4 – Although the impact for the residual risk is within acceptable levels, the likelihood remains high. The internal auditor should report to management and recommend further mitigation procedures. Only those controls that mitigate the risk effectively and efficiently should be included in the engagement work programme. The auditor should recommend the elimination of inadequate controls that do not contribute to the mitigation of the risk.
- Risk number 5 – The residual risk is within the risk appetite. The internal auditor should include the inspection of the controls and other activities that mitigate the risk in the engagement work programme for:
  - their efficiency and effectiveness to mitigate the risk; and
  - if they are acceptable as risk mitigation procedures, the finding should be one of compliance.
- Risk number 6 – Although the likelihood for the residual risk has decreased, it is still not within acceptable levels. The internal auditor should report to management and recommend further mitigation procedures. The auditor should include only those controls in the engagement work programme that

mitigate the risk effectively and efficiently; he/she should recommend the elimination of inadequate controls that do not contribute to the mitigation of the risk.

- Risk number 7 – The residual risk is within the risk appetite. The auditor should include the inspection of the controls and other activities that mitigate the risk in the engagement work programme for:
  - their efficiency and effectiveness to mitigate the risk; and
  - if they are acceptable as risk mitigation procedures, should find them to be compliant.
- Risk number 8 – Although the likelihood level of the residual risk is now acceptable, the impact is still not within the acceptable risk levels. A report should be made to management and further mitigation procedures or the elimination of the activity should be recommended. Only those controls that mitigate the risk effectively and efficiently should be included in the engagement work programme, other inadequate controls that do not contribute to the mitigation of the risk should be recommended for elimination.
- Risk number 9 – The inherent risk is already within the risk appetite, thus management is wiling to accept the risk as it is. It is therefore not cost effective to inspect the mitigation procedures that lower the risk. The auditor should recommend to management that they investigate and eliminate unnecessary, redundant or excessive controls and other procedures (IIA 2009(e):par 10).

The above explains how the risk management process can be used to develop the internal audit engagement work programme. The potential results of using this methodology are the following and are consistent with the newly issued guidance of the IIA (2009(e)) on the use of the risk management process in the planning of the internal audit function's activities:

- All high-risk areas are included in the engagement planning (risks 1 to 8).
- The investigation of controls and other activities mitigating the high risks are automatically included in the engagement work programme, either for in-

depth inspection and compliance, or for suggestions to facilitate improvement.

- Low risk areas could be eliminated entirely, thus not wasting the internal auditor's time and scarce resources and reducing over-controlling (risk 9).
- Recommendations on how to mitigate risks when risks remain high could be made on a timely basis by issuing an interim internal audit report (risks 2, 3, 4, 6 and 8).
- Recommendations could focus on either the lowering of the impact or of the likelihood when additional procedures are needed to mitigate the risk.

The above explanation of how the risk management process can be used to perform a fourth generation internal audit engagement based on risk could be an appropriate aid to not only minimise the internal auditor's efforts, but also provide more focus. Especially in the light of the scarcity of competent internal auditors (refer to section 2.6.3 on p. 119), the effect of the global economic meltdown (refer to section 2.6.5 on p. 123) and the growing complexity of the business environment, this could be a much-needed tool. However, it is important to note that the professional judgement of the internal auditor should never be compromised and due professional care must at all times be exercised (IIA 2009(a):20). For example, if the internal auditor suspects a possibility of fraud or if the controls implemented for risk number eight also perform a preventative control function for collusion, the controls should remain and be included in the engagement work programme.

4.5.6 Conclusion

As the term risk-based internal auditing is fairly new, it seems that the terminology is not used consistently – it is used to describe the audit of the risk management process, planning the internal audit function's activities based on risk, or performing an internal audit engagement based on risks. When looking at the overall evolution of the internal audit engagement process, it seems that risk has been incorporated since the 1990s and beyond. However, it is only since the beginning of the new millennium (2000s) that the risk management process has

been used as a foundation for the planning phase. Even then, all the elements of the risk management process are not fully incorporated and further improvements to streamline the internal audit engagement process are needed. This is especially evident when one reflects on the concern of management regarding over-controlling (refer to section 4.3.3.2 on p. 249), the scarcity of internal audit resources (refer to section 2.6.3 on p. 119), and the threat of internal auditing's scope of activities being too wide (refer to section 2.6.4 on p. 122). Therefore, as discussed in the next section, it is important to study the future of the internal auditors' role with regard to risk, including both the internal audit profession's view, as well as management as one of the most prominent clients of the internal audit function.

4.6 FUTURE OF INTERNAL AUDITING'S ROLE IN RISK

It is important for the profession to ask what the future of internal auditing is to be able to plan ahead. With the growing importance of internal auditing and the modern trend of internal auditors assisting management in accomplishing their objectives, the question arises as to whether internal auditing is generally on the right track, and more specifically regarding corporate governance and risk management strategies, processes and methodologies.

Regarding the future role of internal auditing in corporate governance and specifically risk management, it is important to note that this role will never be stagnant. These processes will evolve and management may need different inputs from internal auditing. Also, what works best for a specific organisation may not be appropriate for another. With this in mind, this section elaborates on the problems that internal auditing faces with regard to corporate governance in general, and risk management specifically. Secondly a few important trends and developments are discussed, including the perceptions of management as the main client of the internal audit function, as well as internal auditors themselves.

4.6.1 Problems experienced by internal auditing

Various studies (Deloitte & IIA (UK and Ireland) 2003; Paape *et al*. 2003; Spira & Page 2003; Gramling *et al*. 2004; Beasley *et al*. 2005; Jackson 2005(a); Gramling & Myers 2006; Sarens & De Beelde 2006(a); Sarens & De Beelde 2006(b); Goodwin-Stewart & Kent 2006(b); Arena *et al.* 2006; Campbell *et al*. 2006; Allegrini *et al*. 2006; Fraser & Henry 2007; IIA Research Foundation 2007; Roffia 2007; PWC 2008(a); Marks 2008:29-30; Ernst & Young 2008; IIA Research Foundation 2009(b)) address concerns regarding the changing role of internal auditing. With reference to risk management, these include aspects such as:

- Top management's lack of understanding of the usefulness of risk management to avoid surprises, and as a result not giving their full support to the process, including to the internal auditors (refer to section 3.7.1.1 on p. 216). This results in a lack of resources available to perform internal auditing tasks properly.
- There has been a lack of management attitude change – management are not doing enough to send out a signal to employees that risk management is important for sound business principles. This could hinder the internal auditor's task when trying to obtain information from said employees.
- The integration of the risk management process efforts into the planning of the organisation as a whole is lacking, including in the annual plan of the internal audit function (refer to section 4.3.2 on p. 242).
- The risk management process is approached qualitatively, producing major differences in the outcome due to, *inter alia*, the capabilities of the organisation, information quality and the probability theory's weaknesses; this results in unreliable information from the risk management process (refer to section 4.6.1.1 on p. 285).
- Internal auditing sometimes plays a leading role in the implementation phase of the risk management framework, this means internal auditing may perform inappropriate activities, such as determining the risk appetite of the organisation (refer to section 2.6.1 on p. 113 for a discussion of the independence of the internal audit function).

- Risk is being divided into and dealt with in segments (silo approach) instead of the organisation focusing on the bigger picture including the ripple effect of a specific risk on other sections, activities and functions of the organisation (refer to section 3.7.1.2 on p. 217).
- Internal auditing sometimes do not have industry-specific knowledge and will therefore not understand the business process sufficiently to be able to make a meaningful contribution to the risk management process (refer to section 4.6.1.2 on p. 286).

Although the above is not a comprehensive list, it does include the most referred to aspects. The 'tone-at-the-top' or management's attitude and philosophy is by far identified as the most concerning reason for the lack of a proper risk management framework, resulting in internal auditing also not implementing risks into their daily activities. However, two further concerns include the use of the qualitative approach when doing a risk assessment – either performed by a risk responsible body and the outcome being used by the internal audit function, or performed by the internal audit function, and the knowledge of the internal auditor with regard to risk-related aspects.

4.6.1.1 Qualitative and quantitative risk assessment

A very important tool for internal auditors is the use of quantitative risk analysis as opposed to the current qualitative approach model used by most internal audit and/or risk management departments. Risk assessment can be carried out using qualitative, semi-qualitative or quantitative techniques (refer to section 3.5.2.3 on p. 198). Quantitative techniques are based on mathematical fundamentals and include interval, ratios, probabilistic, non-probabilistic and benchmarking techniques (Scanfield & Helming 2008:42). Qualitative techniques involve a strong element of professional judgement, whereas semi-qualitative techniques first conduct the risk assessment mathematically (usually very basic techniques such as analytical procedures) and then balance this with qualitative factors (Jackson 2007:40-42).

Bernstein (1996:383) argues that with the rise of risk management, decision makers face two major risks, namely the risk of ignoring a risk or the risk of being deceived by the risk management process. In a study performed by Backlund and Hannu (2002) where three different risk assessment consultants were used on the same activity, the results, being contradictory, indicated that risk assessment could be misleading. Qualitative risk assessment is criticised (Backlund & Hannu 2002:77-80; Emblemsvag & Kjolstad 2002:842; Benson 2007:87) for producing different results due to the capabilities of the role players (such as lacking experience, knowledge and creativity), ignoring the capabilities of the organisation as a whole (such as strengths and weaknesses), and the lack of information quality management.

According to Emblemsvag and Kjolstad (2006:401-406), the greatest advantage of mathematics is its consistency. When scientific mathematical concepts are used to develop statistical models and other tools to determine the risk related to a specific objective, it is normally much more accurate than other methods. Until recently, quantitative techniques were mostly used in financial services organisations as such techniques are difficult to perform and sufficient data and expertise are needed for successful measurement – both these being available in the financial sector (Scanfield & Helming 2008:43). A pure qualitative risk assessment has definite weaknesses and internal auditors and other individuals responsible for risk management have to consider a more scientific approach in identifying, evaluating and measuring, and managing risks (Hespenheide & Funston 2006:13). This will however also result in additional expertise needed.

4.6.1.2 Risk-related knowledge of internal auditors

According to corporate governance guidance (refer to section 4.3.1.1 on p. 234) as well as literature studies (refer to section 4.3.1.2 on p. 239), the most important role that internal auditors should play in the risk management framework is that of providing assurance on the various structures, processes and role players' duties. However, it seems that some parties do have concerns regarding this statement. In studies where management was questioned about the role of internal auditing in risk (Joint Working Group cited in Lemon & Tatum

2003:273; McCarthy & Flynn 2004:21; Fraser & Henry 2007:404; Marks 2008:29), management suggests that internal auditors do not have enough industry knowledge to make a meaningful contribution to the risk management framework, especially the risk management process. This is an even greater concern where the internal auditors are mostly accountants (Fraser & Henry 2007:404) with little or no operational experience. To overcome management's concern, internal auditors should ensure that all parties are aware that they are advisors or assurance providers and not owners of risk (Hespenheide *et al.* 2007:4-5). Although internal auditing has moved away from being purely assurance providers to include the role of consultant (refer to section 2.4.1.1 on p. 71), the performing of certain duties will jeopardise the independence of the internal audit function (Baker 2004(a):18-19; Gramling & Myers 2006:55-56; Fraser & Henry 2007:403). For example, although internal auditors should have a detailed understanding of the organisation's environment, and this includes a thorough understanding of the possible risks threatening the organisation's objectives, it is not the duty of internal auditing to identify or assess a highly technical-specific risk, such as risks related to a chemical process. Therefore, they do not need detailed industry-specific knowledge when evaluating whether the process followed to identify the risk is the most effective. However, there is a definite move to split the risk responsible body (refer to section 3.3.6.2 on p. 179) and the internal audit function as this will overcome the problems of lack of knowledge (which will reside with the risk responsible body) and the jeopardising of the independence of the internal audit function.

In addition, if internal auditing wants to rely on the risk management process and incorporate the outcome into the internal audit function's annual plan and internal audit engagements, internal auditors need to be risk intelligent. Risk intelligence does not necessarily mean being able to list all the risks that the organisation is facing, but merely having a broad understanding of the nature of the environment and related risks to be able to ensure that all major risks are being addressed (Lemon & Tatum 2003:273; Hespenheide *et al.* 2007:8). However, in organisations that are serious about risk management and where internal auditing plays a key role, there seems to be a move to a leaner internal audit function with more experienced and knowledgeable individuals, supplemented by temporary

staff (either in-house or outsourced) with special technical knowledge (Deloitte & IIA (UK and Ireland) 2003:10; Fraser & Henry 2007:405; PWC 2008(b):41). Internal auditors need to take note of the above-mentioned aspect and position themselves accordingly.

4.6.2 Current trends and new developments

Studies (Deloitte & IIA (UK and Ireland) 2003; Paape *et al*. 2003; Spira & Page 2003; Gramling *et al*. 2004; Beasley *et al*. 2005; Jackson 2005(a); Gramling & Myers 2006; Sarens & De Beelde 2006(a); Sarens & De Beelde 2006(b); Goodwin-Stewart & Kent 2006(b); Arena *et al.* 2006; Campbell *et al*. 2006; Allegrini *et al*. 2006; Fraser & Henry 2007; IIA Research Foundation 2007; Roffia 2007; PWC 2008(a); Marks 2008:29-30; Ernst & Young 2008; IIA Research Foundation 2009(b)) have addressed the changing role of internal auditing and have indicated that corporate governance and risk management concepts are, or should be widely incorporated into internal audit activities. The following is a list of the current trends:

- Corporate governance:
  - ensuring that the internal audit function is independent;
  - assisting the audit committee to be effective;
  - reporting audit findings that could have a direct influence on governance aspects; and
  - auditing certain areas such as ethical compliance and culture.
- Risk management:
  - assisting in the risk management process as facilitators and consultants;
  - giving assurance on the risk management process;
  - evaluating the risk management process;
  - incorporating high-risk areas in the audit annual plan;
  - communicating to relevant parties regarding best practices;
  - benchmarking risk management activities;
  - reporting on the stand of risks and controls;

- providing input into a centralised risk database;
- providing assurance that all possible risk exposures are identified and managed; and
- training of employees on risk management strategies and practices.

Although the above are not comprehensive lists but only refer to the trends that are most discussed in the literature, it is clear that they could be improved and extended, especially the current activities of internal auditing with regard to corporate governance. When referring to section 4.2.2 on p. 229, the roles and responsibilities of internal auditing with regard to corporate governance, areas that could also be included in the activities of the internal audit function are the effectiveness of the corporate governance structures (such as board committees) and systems, the adherence or incorporation of governance laws and guidance, and the efficiency with which corporate governance is implemented and managed within the organisation. With regard to risk management, no mention is made of the assurance provided on the overall risk management framework over and above the risk management process referring to structures and other systems. Furthermore, apart from the inclusion of risk into the internal audit function's annual plan no mention is made on how risk can be used to streamline the daily activities of internal auditors.

4.6.3 Expectations of role players

Without internal auditors having a clear understanding of what the board and management want from them, it is difficult for the profession to sell what they already have to offer as well as improve on current activities. The expectations of management with regard to the role and function of internal auditing are fundamentally determined by the standing of the internal audit function within the organisation (refer to section 2.7 on p. 130 for a discussion). According to the study performed in 2003 by Deloitte and the IIA (UK and Ireland), where the views of chief audit executives were compared with chief executive officers, chief financial officers and audit committee chairs, management's perspective on internal auditing is moving in the right direction as 95% of the participating board directors agreed that the overall standing of internal auditing has increased

(Deloitte & IIA (UK and Ireland) 2003:6). This is confirmed by the iKUTU study (2009:107) in SA where top management expressed their extreme satisfaction with their internal audit function by implementing almost all recommendations made by the function. With the improved standing of the internal audit function, the question remains as to what management expects from internal auditing with regard to risk-related aspects and what internal auditing can deliver.

4.6.3.1 Management's expectations

Management has a responsibility to understand the concept and methodology of risk management as well as the benefits it may have for the organisation. They need to take note of who the various role players are (including internal auditing) and what each party's tasks are or should be. They need to understand that while risk taking is an essential part of managing an organisation, the risk management process can assist them in making informed decisions, thus managing risk to optimise the performance of the organisation.

Primarily, management expects internal auditing to create a sufficient level of risk and control awareness (McCarthy & Flynn 2004:20; Sarens & De Beelde 2006(b):238) and support risk management efforts as requested (IIA Research Foundation 2009(b):23). However, recent corporate failures and scandals (refer to section 2.5.2.4 on p. 103) as well as the evolution of corporate governance (refer to section 2.5.2 on p. 87) have put the internal audit profession in the limelight. It is time for senior management and the audit committee to take note of the fact that internal auditors are valuable experts that can assist the organisation with managing risks (McCaul 2006(a):35-36; Campbell *et al*. 2006:44).

As discussed in section 3.7.1.1 on p. 216, the attitude and philosophy of the board and senior management are crucial for the successful implementation of risk-related strategies within the organisation. The specific view of management on risk management concepts as well as their trust in the internal audit function will obviously influence what management expect from their internal audit function. McCarthy and Flynn (2004:20), after exploring by means of case studies and interviews what top decision makers are doing regarding risk, came to the

conclusion that many do understand the important role that internal auditing can play. There is however still a gap between some of the aspects as perceived by internal auditing *versus* management. In studies (Deloitte & IIA (UK and Ireland) 2003:12-14; McCarthy & Flynn 2004:20-22; Sarens & De Beelde 2006(b):187; iKUTU 2009:73,80) where board members and/or senior management as well as internal auditors were interviewed regarding the role of internal auditing in risk aspects, various difference in perceptions emerged, including:

- The role internal auditors should play regarding risk management varies from no role to implementing and managing the risk management process. Internal auditors should inform their boards and senior management as to what the role should be according to the guidance provided by the IIA (refer to section 4.3.1 on p. 234).
- The identification of new business risks is seen by both parties as very important. However, it is important for management to know that it is not the responsibility of internal auditing to ensure that all major business risks are identified. Internal auditors should firstly ensure that the processes implemented by management will intercept all major risks, and secondly, while performing their tasks, focus on identifying additional risks.
- The assurance provided that major business risks are being managed properly is one of the key tasks of internal auditing, and although management is somewhat satisfied that this is being done, it seems that internal auditing needs to improve in this area.
- The use of the internal audit function's knowledge and experience is, according to management, an area of concern as many believe that the function does not have adequate industry knowledge (refer to section 4.6.1.2 on p. 286) to make an ultimate contribution to the management of risk. This seems to be a lack of proper communication between the two parties. Internal auditing's role should not be primarily the identification or even management of the risks, but providing management with assurance that all that is possible is done in the most effective and efficient manner to prevent surprises from happening.

For management to have an understanding of how their internal audit function can optimally contribute to the risk management framework they need to understand the environment. Firstly, management should investigate the effectiveness of the internal audit function. Management need to investigate whether their internal audit function is capable of fulfilling their role in the risk management framework and thus adding value. Thereafter they need to make sure that the function is optimally used in the framework – from a consulting role on assisting in implementing an applicable risk management framework, to an assurance role in providing management with feedback on the effectiveness of the framework. Secondly, management should consider creating a separate risk management section – be it a risk officer, internal steering committee or risk department. With a separate body taking responsibility for risk management, internal auditing will be able to focus on their task, namely providing guidance and assurance that the risk management framework is functioning as it should and therefore is adding value. Lastly, as management should provide input into the internal audit function's annual plan (IIA 2009(a):26), management should consider whether or not the internal audit annual plan incorporates all the high-risk areas identified by the risk management process and will audit these in the near future.

4.6.3.2 Internal auditing's expectations

In a study performed by PWC (2008(b)) on how internal auditors perceive the future of internal auditing in 2012, participants indicated that they foresee that drastic changes will take place. One of the key findings (PWC 2008(b):4) is that internal auditing will move from control assurance (control paradigm) to providing assurance on the effectiveness of risk management (risk paradigm). The CBOK study confirms this belief (IIA Research Foundation 2007:53-56) by identifying emerging trends for the internal audit profession – from anticipated growth in the audit of corporate governance and risk management processes (79.5% of the respondents), to new, improved or additional roles to be played in risk management (66.6%) and corporate governance (52.2%).

With regard to risk management, it was noted that in a number of the studies (Gramling & Myers 2006:54; Sarens & De Beelde 2006(a):70; Goodwin-Stewart & Kent 2006(b):91; Ernst & Young 2007:5; Fraser & Henry 2007:396,401; PWC 2008(b):26) the participants underlined the importance of a separate risk management committee, department or officer in driving the risk management process. These two parties (risk committee/department/officer and internal auditing) should complement one another. This will narrow the role of internal auditing to evaluating the success of the risk body's activities in developing a risk-based culture within the organisation and responding to the high-risk areas. If these processes are reliable, internal auditing can incorporate high-risk areas identified into their annual internal audit function's plan and risk-based internal audit engagements.

It is also noted (Meiselman 2007:40) that internal auditing can add value by suggesting improvement in business processes, one of their core activities, by understanding and being aware of the risks threatening those processes. This will compliment the holistic approach in risk management as discussed in section 3.7.1.2 on p. 217.

An additional point is management's future planning for investing in the improvement of and increasing use of audit tools in the risk management process (Roffia 2007:12; IIA Research Foundation 2007:227-232; PWC 2008(b):31,47; Deloitte & IIA (UK and Ireland) 2008:13), for example, risk-based audit planning, continuous auditing, risk mapping, risk analysis and control self-assessment. These tools can be used by internal auditors in performing their risk management duties as well as risk-based internal audit engagements.

In organisations that lack any or proper risk management strategies (risk immature), internal auditing, true to Practice Advisory 2120-1 (IIA 2009(a):107) will have to educate the appropriate stakeholders (Meiselman 2007:40). Internal auditing will have to take the necessary steps to ensure that the board, the audit committee and senior management are aware that risk management is an integral part of sound corporate governance. The next step will be to share knowledge with and give advice to individual business units on specific risks and

the management thereof, thus improving the overall risk maturity of the organisation.

It is a fact that the business environment is constantly changing and with that the risks threatening an organisation. Internal auditing can play a major role in preventing problems from occurring by communicating emerging risks to the appropriate stakeholders, warning them in advance as well as reviewing the management of key risks by appropriate parties. This is especially the case where no risk department or officer exists, as the internal auditing function can fulfil the role of communicating risk-related aspects.

Lastly, as all the above new developments take place and more organisations implement a risk management process along with internal auditing incorporating risk management strategies into their activities, the lack of skilled risk management professionals will most probably increase (Meiselman 2007:40; PWC 2007:30; Ernst & Young 2007:8; Robert Half International 2007; PWC 2008(a):37-38; Deloitte & IIA (UK and Ireland) 2008:15). Internal auditors will have to position themselves to address this possible shortage, especially in these times where the global financial crisis could have an effect on the profession (refer to section 2.6.5 on p. 123).

4.6.4 Conclusion

The above indicates the problems, areas of concern and possible future trends identified by internal auditors and management on risk management. It could be possible that management have a totally different view on where they see internal auditing with regard to risk management within the next few years. However, although there has been an increase in legislation and other documents addressing corporate governance aspects, including risk management and internal auditing, over the last few years, whether this has affected day-to-day business activities is another question. This is evident by the number of business scandals involving executives as published by the US Securities and Exchange Commission (Waring 2006:35-37). Internal auditors need to be proactive in the

fight to improve corporate governance and risk management within their organisations. This could include aspects such as:

- the IIA taking a stand on the independence of the internal audit function;
- internal auditors offering their services with regard to awareness programmes to various corporate governance stakeholders; and
- individual internal auditors starting to demand the establishment of various programmes that will enhance corporate governance such as ethics training and whistler blower protection programmes.

If internal auditing is assisting in the risk management process, a priority is to ensure that management identifies the most critical risks threatening the organisation. Internal auditing will also need to keep up to date on these possible risks and incorporate them in their audit activities.

4.7 SUMMARY AND RELEVANCE TO THE STUDY

This chapter deals with the role that internal auditing should play with regard to corporate governance in general, and more specifically with the management of risk.

With regard to corporate governance, internal auditing's main objective is to assist the board of directors with the execution of their duties and responsibilities by mainly providing assurance on certain activities. Although this is currently the case, it seems that the activities performed by the internal audit function could be even further enhanced.

- Internal auditing should provide:
    - guidance with the establishment and/or implementation of governance structures as stipulated by corporate governance codes; and
    - assurance on implemented governance structures.

With regard to the management of risk, the IIA identifies three areas where internal auditing should either provide assurance or incorporate risk into their activities. The first area is the risk management framework:

- The internal audit function should provide assurance on the risk management framework.
- This includes either the auditing of the risk management process, or being actively involved, or managing and coordinating the process on behalf of management (internal audit should, however, not take responsibility for the process).
- If the framework (including the risk management process) is not suitable or effective for the management of risks for the organisation as a whole, internal auditing should advise the board on how to improve the framework and/or process.
- Although the IIA has provided their members with some form of guidance, it seems that:
    - it lacks guidance on the risk management framework; and
    - the guidance is not always adhered to by the IIA's members – inappropriate activities are performed by some members.
- The lack of knowledge and skills possessed by internal auditors with regard to risk management and knowledge of the business are hindering the optimisation of the role that they could play.
- This is especially true for risk management in the public sector of developing countries.

Although not included in the scope of this study, the second area, namely the annual plan of the internal audit function's activities based on risk, is briefly mentioned:

- The outcome of the risk management process should be incorporated into the annual planning of the internal audit function's activities, especially the strategic high risks identified.

- The audit universe (a list of all possible auditable engagements) should focus on the high-risk areas identified by management during the risk management process.

The third area is where risk management practices are incorporated into the performance of an assurance engagement. Although the guidance provided by the IIA is insufficient, the following can be concluded:

- Internal auditors have to take note that there is a new way of auditing, by incorporating the management of risk into their engagement process (forth generation auditing).
- This is best introduced in the planning phase of the engagement.
- When comparing the steps in the risk management process with guidance provided by the IIA on the internal audit engagement planning, it seems that this structured process (used by management to mitigate risks) is ideal as a basis for a risk-based internal audit engagement.
- For the optimisation of the above, the following should be taken into consideration:
    - the organisation should have a high level of risk maturity;
    - the internal audit function has audited the risk management process and is placing reliance thereon;
    - certain steps in the risk management process should be performed outside the internal audit function, for example, by the risk department;
    - these steps should be properly documented, for example, in a risk register; and
    - the risk register should include both strategic-level assessments as well as operational-level risk assessments (thus also for the activity under review in the internal audit engagement scope).

When comparing the current use of the risk management process as a basis for the risk-based internal audit assurance engagement, the following weaknesses have been identified:

- The internal auditor does not always rely on the risk identification and the assessment thereof by another party (such as the risk department), but re-performs the whole process.
- Risk as the loss of opportunity as a form of risk is not always included by the internal auditors when identifying risks.
- The difference between the inherent risk and the residual risk should be the starting point of the engagement planning, but is sometimes ignored.
- The risks identified in the activity under review could have an effect on another business unit and process. Risks should therefore be viewed holistically, but this is currently not always the case.
- Controls are mostly used as the means to mitigate risks, but other forms of procedures could be more effective and efficient.

To address the above weaknesses, the internal auditor should ensure the following as part of a risk-based internal audit engagement model:

- Use the objective setting for the activity under review as performed by the risk department.
- Use the identification of inherent and residual risk-levels as determined by the risk department. If needed or appropriate, identify further risks.
- Use the assessment in terms of impact and likelihood as determined by the risk department.
- Use the risk appetite levels as determined by the board of directors.
- Include the following in the engagement planning:
    - controls that mitigate the inherent risks within acceptable levels;
    - areas where the difference between the inherent and residual risks are high (focus only on the controls that do make a difference); and
    - unacceptably high inherent and/or residual risks where management's attention and action is urgently required.
- Use professional judgement in areas where the inherent risk is already low, for example, where fraud is suspected.

Although a few problems are experienced by the internal audit profession when it comes to risk management, two are highlighted, namely:

- The complexity of the quantitative tools and techniques that can be used during the risk management process poses a difficulty.
- The risk-related knowledge of internal auditors when providing assurance on the risk management framework and process is not always sufficient.

It seems that the expectations that management and internal auditing have for the role that the latter should be playing in the management of risk, sometimes differ. However, it does seem that both agree that internal auditing must be involved in this process and should incorporate it into their daily activities, whether performing a risk-related specific audit engagement (such as the auditing of the risk management process), or incorporating the management of risk into the planning of their audit engagements. The next chapter investigates the perceptions of the chief audit executive of a risk mature organisation when it comes to performing a risk-based internal audit assurance engagement. These views are used to adapt and further refine the preliminary risk-based internal audit model as developed in this chapter.

CHAPTER 5
RESEARCH RESULTS OF THE EMPIRICAL STUDIES: RISK MATURITY, REFINING THE RISK-BASED INTERNAL AUDIT ENGAGEMENT MODEL AND TESTING THE MODEL

5.1 INTRODUCTION

In this chapter, the results of the three empirical studies are summarised as well as briefly discussed. The results are discussed in the context of the literature study as documented in Chapters 2 to 4 and the empirical methodology as discussed in Chapter 1 – as such, references are continuously made to sections within these chapters.

As reflected in the discussion on the research methodology under section 1.8.4.2.1 on p. 44, the first empirical study investigated the true status of risk management within certain SA organisations, also referred to as the level of risk maturity of the organisation. The objective was to identify organisations that are risk mature as this is one of the pre-requisites for an internal audit function to be able to use the risk-based internal audit model (refer to section 4.5.3.1 on p. 264). The research results consist of the information obtained from the application of a pre-developed risk maturity model (adjusted for SA corporate governance requirements) on the disclosure of organisations regarding their risk activities, including annual financial statements, information obtained on the organisations' websites, and information obtained on the McGregor databases.

The second empirical research study is explained in section 1.8.4.2.2 on p. 48. The objective was to obtain input from chief audit executives on the risk-based internal audit model that was developed after studying the literature (refer to section 4.5.5 on p. 274). The research results consist of information that has been obtained through personal interviews of chief audit executives in the top five risk mature organisations, as determined in the first empirical study, in both the SA private and public sectors.

The third empirical study consists of a case study that was performed to test the risk-based internal audit model as described in section 1.8.4.2.3 on p. 51. The main objective of this empirical study was to identify whether the implementation of the model ensures a more effective and efficient internal audit engagement by performing less audit procedures during the execution of the engagement, but at the same time identifying all the significant audit findings. Note that a confidentiality agreement was signed and that the organisation that was used to conduct the case study may thus not be identified.

Lastly, the results of the second as well as the third empirical studies are used to refine the preliminary model that was developed and is described in Chapter 4.

5.2 STATUS OF RISK WITHIN SOUTH AFRICAN ORGANISATIONS

As discussed in section 3.6 on p. 205, risk maturity reflects on the various elements of the risk management framework that has been effectively identified, implemented and applied by an organisation. Thus, it refers to the risk management approach that has been adopted and applied, as planned, by the management of a specific organisation. Various institutions have developed a risk maturity model that assists organisations in determining the level of their maturity (refer to table 3.5 on p. 209 for a comparison of some of these models). In the first empirical study (refer to section 1.8.4.2.1 on p. 44– Objective) one of these models was used to determine the risk maturity of selected SA organisations. The process followed during the execution of the empirical study, and the results of the study are discussed in the context of the literature.

5.2.1 Use of a risk maturity model

After comparing seven models (refer to section 3.6.2.1 on p. 208) with the criteria as set by the Capability Maturity Model (refer to section 3.6.2 on p. 207), the model developed by RIMS Inc. (2006) was chosen as the most comprehensive and appropriate for the purpose of this study. However, the model was developed for all RIMS members on a global scale. The model was therefore adapted to suit SA corporate governance requirements as per the second King Report (IOD

2009), and to address the limitations identified after the comparison of all the models.

5.2.1.1 The Risk and Insurance Management Society Incorporated model

In section 1.8.4.2.1 on p. 44 – Methodology followed, the RIMS model is briefly introduced. It consists of five steps or levels (refer to Annexure B on p. 459) ranging from *ad hoc* implementation of risk management framework elements (step 1) to the optimisation of risk management within the organisation (step 5). The model identifies six criteria within the risk management framework (refer to Annexure C on p. 460) and links deliverables to each criteria (refer to Annexure D on p. 463) as well as attributes within the different levels (refer to Annexure E on p. 466). After comparing seven risk maturity models, and identifying the common criteria used (refer to section 3.6.2.2 on p. 211), two further criteria were added to the six of the RIMS model (refer to section 3.6.3 on p. 213), namely reporting and communication, as well as internal auditing as assurance providers. Deliverables for the five steps of these two areas were developed by consulting various risk management guidelines (refer to section 3.3.4 on p. 163), but mainly focusing on the guidance as stipulated in the second King Report (IOD 2002). The reason for using the guidance in the second King Report and not the third King Report is that the empirical study was conducted early in 2009 and the third report was not yet available at that time.

5.2.1.2 Adapted for South African corporate governance requirements

As mentioned, RIMS developed their model for their nine thousand six hundred risk management professional members globally. In SA, corporate governance guidance and legislation includes risk management (refer to sections 3.3.4.2 on p. 165, 3.3.4.2.1 on p. 170, 3.3.4.2.2 on p. 171 and 3.3.5.2 on p. 175 – SA Government). It was therefore appropriate, as SA organisations were to be tested against the model, to adapt the deliverables to include SA-specific guidance and legislation.

5.2.1.3 Final risk maturity scorecard

The five steps (levels) and the eight criteria (attributes) that were used in the model are listed in Annexure F on p. 474, the risk maturity model scorecard. The eight criteria with the five levels provide forty deliverables, with each carrying a weight of five points – the maximum total score that any one organisation can obtain is thus two hundred. The minimum level for risk maturity is suggested to be level three (repeatable) as the deliverables listed in this step suggest that a level of risk management activities exists that would be useful to the internal auditor. Level one (*ad hoc*) and level two (initial) have too limited deliverables. Therefore, risk maturity is calculated at a hundred and twenty (eight criteria x level three x weight of five).

5.2.2 Empirical study's scope and limitations

The overall scope and the limitations of the study are discussed in section 1.8.3 on p. 42. However, further aspects now need to be mentioned. Firstly, due to the fact that both the private sector and the public sector were included in the study (wide population), time and resource constraints, and more than one empirical study being performed, only the top forty companies listed on the JSE Limited for the private sector and all thirty seven national government departments as on 4 June 2009 for the public sector were investigated. The decision to choose these specific organisations was a carefully considered one (refer to section 1.8.4.2.1 on p. 44– Sample) and, on average, the group of organisations probably includes those within SA with the highest risk maturity levels.

Secondly, as seventy-seven organisations' risk maturity had to be determined, it would not have been feasible to perform an in-depth investigation into the risk maturity level of each organisation. Two sources were used to obtain the relevant information, namely the Internet websites of the various organisations, and the McGregor BFA database. This limited investigation could result in certain information not being taken into consideration while determining the risk maturity level as it can be assumed that not all the information for every organisation was available or disclosed. This limitation is substantiated by the study performed by

Marx (2008:452-455) where information obtained via empirical research is compared with organisations' annual financial report disclosures. The comparison reveals that not all functions, activities, duties, etc., that are in place are reported and disclosed, the users of the research information may thus arrive at conclusions that are not entirely justified. This limitation was minimised by including a discussion on the risk maturity score of the organisation during the interviews performed in the second empirical study. It has to be borne in mind though, that such extra information obtained could be incorrectly interpreted by the analyser or information could have been presented in such a manner that the organisation is perceived to be risk mature but in fact is not.

5.2.3 Risk maturity score

The results of the risk maturity scorecard for each organisation are listed as Annexure G on p. 477 (Private sector) and Annexure H on p. 479 (Public sector). Only ten of the forty public sector organisations were not risk mature (score < 120), whereas not one of the national government organisations was scored as risk mature (score ≥120). One of the government departments, SA Secret Services, had no information available on the Internet, and was therefore excluded from the study (only thirty six organisations were therefore part of the public sector sample). The low scores of the government departments could be as a result of disclosure guidelines as described by the Treasury Department (SA – National Treasury 2010), or due to the fact that guidance on risk management, although addressed in public sector legislation, is not very prescriptive (refer to section 3.3.4.2.2 on p. 171). Although not risk mature, as described in section 1.8.4.2.2 on p. 48 – Population and sample, these organisations were included in the second empirical study, mainly to determine why their risk maturity scores are so low.

The top five organisation scores for each sector that were included in the second empirical study are (alphabetical):

- **Private sector:**
  - ABSA Group Limited (195/200)
  - Impala Platinum Holdings Limited (170/200)
  - Investec PLC (165/200)
  - Old Mutual PLC (170/200)
  - Telkom SA Limited (170/200).

- **Public sector:**
  - Department of Arts and Culture (100/200)
  - Department of Public Service Commission (95/100)
  - Department of Science and Technology (100/200)
  - Department of Social Development (95/100)
  - SA Revenue Services (115/200)
  - Public Administration Leadership and Management Academy (105/200).

Further analysis (refer to table 5.1 below) reveals that on average (*M*) the private sector is risk mature (130.625/200) whereas the public sector is risk immature (66.25/200).

Table 5.1: Analysis of data on risk maturity

Nr	Attributes/Criteria	Private sector Mean (*M*)	Public sector Mean (*M*)
1	Organisational culture	2.25	1.64
2	Involvement in strategy setting	3.55	1.86
3	Risk management policy setting	3.53	1.78
4	Risk management process/framework	3.63	1.67
5	People/staff	2.35	1.14
6	Risk management performance measure	3.4	1.56
7	Internal auditing	3.58	1.83
8	Reporting/communication	3.88	1.78
TOTAL WEIGHED SCORE (total score x 5)		**130.625**	**66.25**

The area that has the lowest maturity levels in both the sectors is the 'people or staff' (referring to individuals that are equipped and supported to manage risk

well), followed by 'organisational culture' (referring to the degree of executive support for formalised risk) for the private sector, and 'risk management performance measure' (measuring the success of risk management) for the public sector. The lack of management's commitment with regard to risk management and the effect thereof on the employees' attitude are discussed in detail in section 3.7.1.1 on p. 216.

5.2.4 Conclusion

The results of the empirical study indicate that the risk management framework for the private sector in general is perceived as being established.

For public sector organisations, the current status of the establishment of a risk management framework is a concern. Whether all the information is not available on the Internet is debatable, as the various websites of the national government departments seem regularly updated and overall, informative. Therefore it was decided to develop a separate questionnaire (refer to section 1.8.4.2.2 on p. 48 – Population and sample) for the public sector with the main objective to try and get an understanding as to the reasons why the organisations in this sector are not risk mature and how this impacts on internal auditing.

In the next section, the second empirical study's methodology is explained and the results of the interviews with participating organisations' chief audit executives are provided.

5.3 OBTAIN INPUT INTO THE RISK-BASED INTERNAL AUDIT MODEL

The second empirical study's main objective (refer to section 1.8.4.2.2. on p. 48 – Objective) was to obtain input from the chief audit executives of the participating organisations concerning their understanding of the role of internal auditing in the overall management of risks, leading to the refining of the preliminary model (refer to section 4.5.5 on p. 274). Only risk mature organisations were included in the sample as it is not possible to apply the model in a risk immature organisation (refer to section 1.8.4.2.2 on p. 48 – Population and sample). However, the

results of the first empirical study indicated a material difference between the top five private and top five public sector organisations. This necessitated the development of separate questionnaires for the two sectors. In this section, the motive for the inclusion of certain topics during the development of the questionnaires, the refining of the questionnaires, the empirical study's scope and limitation, as well as the results of the interviews are provided and briefly discussed. The final interpretation of the results, conclusions and recommendations are discussed in the next chapter.

5.3.1 The development of a structured interview schedule

Two structured interview schedules (refer to Annexure I on p. 481 – Private sector and Annexure J on p. 491 – Public sector) were developed to ensure that the face-to-face interviews were free of bias (Mouton 2005:106). Further advantages linked to this type of data gathering include, *inter alia*, (Leedy & Ormond 2005:184-185; Saunders *et al*. 2007:354-360):

- high confidence that the right person has responded;
- the likelihood of the contamination of the respondent's answers is low;
- open and closed questions can be included; and
- the respondent's participation is enhanced.

In section 1.8.4.2.2 on p. 48 the objectives of the interviews are listed. In the rest of this section, each of these are discussed in the context of the literature review (refer to Chapters 2 to 4) and the structured interview schedule layout (refer to Annexure I on p. 481 and J on p. 491).

5.3.1.1 The relevance and importance of risk management for the organisation and the internal audit function

To determine whether internal audit functions incorporate risk-related aspects into their activities, it is first necessary to understand what risk concepts the organisation have implemented, as well as how internal auditing is involved in

these. According to the literature (refer to Chapter 2) the standing of the internal audit function within the organisation has an effect on how the function is perceived and ultimately utilised, including the incorporation of internal auditing into the overall risk management framework.

Aspects that affect this standing include, *inter alia*:

- the effectiveness and efficiency of the function (refer to section 2.7 on p. 130);
- the structure of the function (refer to sections 2.4.2 on p. 75 and 2.7 on p. 130);
- the independence of the function (especially the reporting lines), including an independent audit committee (refer to section 2.6.1 on p. 113);
- recognition obtained by other role players (refer to section 2.5.3 on p. 106); and
- the appointment of competent and skilled employees, especially within certain specialisation fields (refer to sections 2.6.3 on p. 119, 2.4.3 on p. 79 and 2.6.6 on p. 126).

With the extension of the role of internal auditing within the risk management framework as proposed by the third King Report (refer to table 3.2 on p. 166), it is clear that the internal audit function's role has to evolve. This is also substantiated by the guidance as provided by the IIA (2004). Some of the concerns listed above are addressed in section 1 of the questionnaire (refer to questions 1.5, 1.6, 1.7, 1.8, 1.12, 1.13 in Annexure I on p. 481 and J on p.491).

A second factor that has an effect on the role that internal auditing plays within the risk management framework is the existence as well as responsibilities of certain parties within the organisation's framework (refer to section 3.3.6 on p. 177). As discussed in Chapter 3, the incorporation of corporate governance concepts is unique for a specific organisation. This is also true for the risk management framework. Questions 1.9, 1.10, 1.11 and 1.14 in Annexure I on p. 481 and J on p. 491 briefly address this aspect.

The management of risk is ultimately the responsibility of the board of directors (refer to sections 3.3.4 on p. 163). However, two board committees may assist the board with the execution of these responsibilities, namely the risk committee and/or audit committee. The literature identifies two areas where these committees are involved in the management of risk. Firstly, the risk committee (refer to section 3.3.6.1 on p. 177), or in the absence of such a committee the audit committee (refer to table 3.2 on p. 166), should review and report on the overall effectiveness of the risk management framework, including whether key risks are appropriately addressed. Secondly, the internal audit function should assist the audit committee with the duty (refer to section 4.2.2 on p. 229) of providing assurance that risks are appropriately mitigated (refer to table 3.2 on p. 166). Furthermore, internal auditing should provide independent assurance on the integrity of the risk management framework by issuing a written assessment to the board (refer to table 3.2 on p. 166 and section 4.3.1 on p. 234). From the literature it can be concluded that the board of directors takes comprehensive responsibility for risk management, but is supported, *inter alia*, by its board committees and assisted by various parties, including the internal audit function. It is thus important to understand what type(s) of coordination and communication exists between these parties. This is addressed in question 1.15 in Annexure I on p. 481 and J on p. 491.

With regard to adherence to the IIA *Standards* in respect of risk management, the literature indicates that not all of the guidance is strictly followed (refer to sections 1.2.4.7 on p. 11 – general adherence to the IIA *Standards*; 4.3.1.2 on p. 239 – risk management; 4.3.2.2 on p. 244 – annual planning of the internal audit function's activities; 4.3.3.2 on p. 249– risk-based internal audit engagements). This is because the *Standards* are not legislation to organisations and, therefore, not necessarily fully implemented by each organisation. Part 2 of the questionnaires (refer to Annexure I on p. 481 and J on p. 491) was set to determine a specific organisation's scope of adherence as this could influence the role that internal auditing might play. It should also be noted that although certain activities could be regarded as basic requirements for one organisation, the same activities might not be as important to another. Since the national departments' respondents indicated that these departments are risk immature

(refer to Annexure J on p. 491), an additional section was added in this sector's questionnaire enquiring as to when full adherence could be expected – this also took into account that the Treasury Regulations (SA – Treasury Regulations 2005:par 3.2.6) enforce the *Standards* on government organisations. Lastly, the *Standards* have recently been updated (January 2009) due to new developments and it could be that as individuals are becoming more familiar with the concept, more guidance on risk management is required.

Although SA corporate governance guidance and legislation (refer to sections 4.3.1.1.2 on p. 238, 4.3.2.1.2 on p. 244 and 4.3.3.1.3 on p. 249) supports the fact that internal auditing should be part of risk management (refer to table 3.2 on p. 166), not much other guidance specifically address this aspect. Furthermore, the literature identifies various aspects that have, and still do influence the holistic incorporation of risk management into the business environment (refer to Chapter 2). Part 3 of the questionnaires (refer to Annexure I on p. 481 and J on p. 491) enquired whether the interviewee considers internal auditing to be part of risk management, and if so, has the internal audit function's involvement increased, or is the interviewee anticipating a further increase due to certain factors. Lastly, for the public sector, an additional question was included to identify the specific aspects that had, or will have an influence on the role of internal auditing within risk management.

A position statement issued by the IIA (2004) identifies the activities that should be performed by the internal audit function with regard to risk management, both the core activities and the consulting activities that should be performed with safeguarding. In addition it identifies the activities that are not suitable for the internal audit function (refer to figure 4.1 on p 237). However, the literature (refer to section 4.3.1.2 on p. 239 shows that this guidance is not always adhered to and that, with the many changes affecting (refer to sections 2.4 on p. 70 and 2.5 on p. 84), as well as threats to (refer to section 2.6 on p. 113) the profession, the role that internal auditing plays within the risk management framework is, and should not be stagnant. Questions 4.1 and 4.2 (refer to Annexure I on p. 481 and J on p. 491) were set to determine the current and possible future responsibilities the internal audit function has with regard to the risk management framework,

both in term of consulting activities and providing assurance. For the public sector, questions 4.3 and 4.4 (refer to Annexure J on p. 491) addressed factors that may hinder the internal audit function from providing the necessary service.

The last area (refer to part 5 of the questionnaires in Annexure I on p. 481 and J on p. 491) related to risk concepts is the implementation of a risk management process (refer to section 3.5 on p. 191. As this is essential for the performance of a risk-based internal audit assurance engagement (refer to section 4.5.4 on p. 268), the questions were structured in such a manner that, apart from the role that internal auditing might play in this process, the necessary elements (refer to section 4.5.3 on p. 264) needed to ensure that internal audit engagements are based on the second COSO (2004) model (refer to the evolution of internal audit engagements – tables 4.2 on p. 260 and 4.4 on p. 269) could also be determined.

5.3.1.2 Determine whether the internal audit function includes risk concepts in its activities

The internal audit function should address risk in their activities by incorporating high strategic risks into their annual plan (discussed in this section) and performing risk-based internal audit engagements (discussed in the next section). As mention in section 4.3.2 on p. 242, this duty of the internal audit function is not part of the scope of this study. However, as supported by the literature (refer to sections 4.3.2.2 on p. 244 and 4.5 on p. 258), the establishment of a risk-based annual plan is the first step for internal auditing to incorporate risk into their activities. It is therefore more likely that when internal audit functions do incorporate risk into the annual planning they will also incorporate risk when performing an internal audit engagement. Part 6 of the questionnaires (refer to Annexure I on p. 481 and J on p. 491) briefly investigated whether risk is incorporated into the annual planning of the internal audit function, specifically also whether the outcome of the risk management process is used as a basis for the plan (refer to section 4.3.2.1.1 on p. 241). For the public sector questionnaire, both the PFMA (SA – 1999:S38) and Treasury Regulations (SA – National Treasury 2005:3.2.1,3.2.7) as well as the third King Report (IOD 2009:94)

guidance was used. For the private sector, only the King Report (IOD 2009:94) guidance was used.

5.3.1.3 Determine whether the internal audit function incorporates risk-based planning in their internal audit engagements

Although not many literature sources could be obtained specifically addressing risk-based internal audit engagements (refer to section 4.3.3.2 on p. 249), it was concluded that the planning of an internal audit engagement should be based on risk (refer to table 4.1 on p. 256 and figure 4.2 on p. 257). Additionally (refer to section 4.5.3.1 on p. 264), the risk maturity of the organisation is vital to the successful implementation of risk-based internal audit engagements (this was addressed in the first empirical study and the maturity score is confirmed with question 1.16 in Annexure I on p. 481 and J on p. 482 – also refer to table 5.2 on p. 316 for the results). Lastly, with reference to the evolution of internal audit engagements, it can be assumed that the second COSO (2004) model is essentially the basis for a risk-based internal audit engagement (refer to tables 4.2 on p. 260 and 4.4 on p. 269). However, it is evident from the literature (refer to table 4.5 on p. 272) that this is not always the case. In part 7 of the questionnaire (only for risk mature organisations – Annexure I on p.481), the performance of a risk-based internal audit engagement according to the second COSO (2004) model was investigated (question 7.1 in Annexure I on p. 481), including the obtaining of information (question 7.2 in Annexure I on p. 481), the starting point (questions 7.3 in Annexure I on p. 481), and specific inclusions (question 7.4 in Annexure I on p. 481) as identified by the literature (refer to section 4.5.4.2 on p. 270).

5.3.1.4 Obtain input into the preliminary developed risk-based internal audit engagement model and adapt the model accordingly

Section 4.5.5 on p. 274 (including figures 4.3 on p. 277 and 4.4 on p. 279), details the development of a preliminary risk-based internal audit assurance engagement model based on the aforementioned literature. In part 8 of the questionnaire (only for risk mature organisations – Annexure I on p. 481), the model was briefly

explained to the interviewee, where after input was obtained on whether the model could be used in the planning of an internal audit engagement and the effect it could have on the efficiency and effectiveness of the internal audit function.

5.3.2 Refine the questionnaires

Two preliminary questionnaires were set with input from audit researchers (De Jager 2009; Plant 2009; Fourie 2009), internal audit practitioners specialising in risk management (Du Plessis 2009(a); Smit 2009) and a statistician (Owen 2009), regarding the content of the questionnaires as well as refining the way in which questions were set. The questionnaires were adapted and the final questionnaires were edited by a language expert for consistency and clarity of the way questions were set.

5.3.3 Empirical study's scope and limitation

The overall scope and limitation of the study is discussed in section 1.8.3 on p. 41. However, for the purpose of this empirical study, further aspects need to be mentioned. Firstly, the methodology followed as well as the population and sample took into account the scope and limitation of this empirical study as discussed in section 1.8.4.2.2 on p. 48.

Secondly, with the exception of Old Mutual, only chief audit executives or managing partners (in the case of an outsource function) were interviewed. Old Mutual was undergoing a restructuring exercise at the time and the head of internal auditing for the SA office had recently resigned, therefore it was decided that the Quality Assurance Department as well as the chief operating officer of the group internal audit function should be involved in the research (Thiart 2010). For the other interviews, although it would have been much easier to interview other senior members of the internal audit function due to the non-availability of the chief audit executive, this stipulation was not compromised. The interviews were kept to between one and two hours in duration due to this fact.

Thirdly, the fact that only five organisations were chosen per sector has proven to be sufficient for the private sector. Holistically, the same type of information was obtained at the five organisations for this sector and more interviews would most probably have revealed the same information. However, for the public sector, it should be noted that although the top five organisations were included, due to restrictions placed by the Commissioner on communication with the public (Singh 2010), the SA Revenue Services had to be replaced by the next department on the maturity list (refer to Annexure H on p. 479). The Public Administration Leadership and Management Academy was unwilling to participate in the study and was also replaced by the next risk mature organisation. Furthermore, as risk management had, at the time, only recently been introduced in most of this sector's organisations, it seemed that new developments were constantly taking place. This could mean that for each organisation different factors have, and still are influencing its risk maturity. It is probable that not all possible factors were identified during the five organisations' interviews. Aspects identified during the interviews include the over-exaggeration in the financial statements on the true status of risk maturity, changes that have occurred during the last six to twelve months in the implementation of elements of the risk management framework, management not fully understanding and appreciating the role of risk management, and individuals in risk positions very new to, and ignorant of their duties, to name but a few. It should, however, be noted that this sector was only included to try and get an understanding of the reasons why the organisations are not risk mature and how this affects the internal audit function's activities (refer to section 1.8.4.2.2 on p. 48 – Population and sample), and did not influence the development of a risk-based internal audit model.

In the fourth place, a document explaining the terminology such as risk management framework and risk management process, as well as the specific organisation's risk maturity scorecard were provided to the interviewee and explained before the interview took place.

In the fifth place, the use of a structured interview proved to be the best method to follow as the dialogue led to in-depth discussions. Furthermore, with regard to

the explanation of the use of the model, individuals would not have grasped the methodology without a one-on-one discussion.

Lastly, the average risk maturity score for the attribute 'internal audit' (refer to attribute 7 in table 5.1 on p. 305) is 3.58 for the private sector respondent organisations and 1.83 for the public sector respondent organisations. The overall risk maturity score per attribute for the private sector respondent organisations is 3.27 (refer to the total in table 5.1 on p. 305 – 130.625 / 8 attributes / 5 per score) and for the public sector respondent organisation 1.66 (refer to the total in table 5.1 on p. 305 – 66.25 / 8 attributes / 5 per score). These scores indicate that the internal audit function's risk maturity attribute (attribute number 7 in table 5.1 on p. 305) is above average compared to the other attributes within each of the sectors. Furthermore, with reference to the scores of the ten organisations that were included in the second empirical study, the attribute 'internal audit' was even higher with a score of 4.6 for the private sector organisations and 3.4 for the public sector organisations, confirming that these chief audit executives were in the best position to add the most value to the development of the risk-based internal audit model (for the private sector) or to understanding the limitations of the role of internal auditing regarding risk management (for the public sector).

5.3.4 Discussion of results

In this section, the results of the interviews are summarised and briefly discussed in the context of the research questions (refer to section 1.8.4.2.2 on p. 48). As the private and the public sectors had separate questionnaires, the discussion will distinguish between the two sectors (five results per sector). The interpretation of the results as well as possible comparisons between the two sectors will be discussed in the next chapter.

Before the results are discussed in detail, it is important to mention that the risk maturity score (refer to section 5.2.3 on p. 304) of each organisation was verified during the interview by discussing the specific organisation's scorecard (refer to question 1.16 in Annexure I on p. 481 and J on p. 491). The results are provided in table 5.2 on p. 316.

Table 5.2: Risk maturity score agreement

Private sector		Public sector		
Agree	**Disagree**	**Agree**	**Disagree**	**Unsure**
5	0	1	1	3

From the above it appears that the chief audit executives of the private sector organisations are not only up-to-date with the risk maturity of the organisation, they agree with the information published in documentation made available to the general public (the first empirical study was performed using information obtained from the Internet and other publicly-available databases).

For the public sector, only one chief audit executive agreed with the score. Others felt that the score should be even lower, or they were unsure of whether it was a true reflection, or felt that although it was correct according to the published information, it should be higher as things had changed dramatically for the better over the last six months to a year.

5.3.4.1 The relevance and importance of risk management for the organisation and the internal audit function

As mention in section 5.3.1.1 on p. 307, it is first important to understand the structure and functioning of the organisation to be able to understand how risk is embedded into the day-to-day activities of the organisation, and more specifically the internal audit function. The results obtained through the interviews on a few of the most important factors as identified by the literature study and discussed in section 5.3.1.1 on p. 307, are provided in this section.

5.3.4.1.1 Factors influencing the standing of the internal audit function

- **Structure of the function and types of activities performed**

The structure of the internal audit function has a direct influence on which activities are performed and how they are performed. One aspect of this structure, as debated in section 2.4.2 on p. 75, is the implementation of either an

in-house function, the use of an outsourced consultant, or a combination of the two (co-sourcing). For sound corporate governance, if a function is outsourced, senior executives must be custodians of the structuring, functioning and independence of the function (refer to table 2.5 on p. 99). An additional aspect concerns the performance of consulting engagements as well as assurance engagements (refer to section 2.4.1.1 on p. 71) as this could also affect the independence of internal auditing (refer to section 2.6.1 on p. 113). Table 5.3 below provides the results on the structure of the internal audit function and types of activities performed.

Table 5.3: Structure and type of activities of the internal audit function

Type of activity	Private sector		Public sector	
	Number of respondents	**Mean (*M*)**	**Number of respondents**	**Mean (*M*)**
In-house consulting	3	5.4	3	6
Outsourced consulting	1	3	2	2.2
In-house assurance	5	78	4	55.4
Outsourced assurance	3	13.6	4	36.4
TOTAL		100		100

When referring to the debate on whether internal audit functions should perform assurance engagements or consulting engagements (refer to section 2.4.1.1 on p. 71), the effect on the independence of the function (refer to section 2.6.1 on p. 113), the value that both these add to the organisation (refer to section 2.4.1.2 on p. 73), and the theory of internal auditing (refer to section 2.3 on p. 63) support the fact that assurance engagements are still the main priority of the internal audit function. The above results support this fact with only 8.4% of the private sector's and 8.2% of the public sector's audit activities being consulting engagements, with the majority of the activities (91.6% and 91.8%, respectively) focusing on assurance engagements.

With regard to assurance activities, the private sector respondents indicated a very low rate for outsourcing, namely 13.6%. This could be as a result of the fact that most of the private sector organisations that participated in the study are regulated by their specific industry not to outsource.

Respondents from public sector organisations indicated that on average 36.4% of their assurance engagements are outsourced to an external service provider. This tendency could be explained (refer to sections 2.4.3 on p. 79 and 2.6.3 on p. 119) by:

- the size of the internal audit function, with an average of 5.4 staff members per responding organisation (refer to tables 5.4 on p. 319); and
- the shortages of competent internal auditors (refer to table 5.5 on p. 320), especially those holding a professional qualification.

- **Internal audit function within the organisational structure**

With regard to whether the internal audit function is a separate department or part of another department, for example, the financial department, three of the five private sector organisations and four of the five public sector responding organisations indicated that the internal audit function operates as a separate function. The remaining respondents indicated that the internal audit function is structured within the financial section of the organisation (two private sector respondents) and the governance section (one public sector respondent). The two organisations that indicated that their internal audit function is situated within the financial section could give rise to concern regarding the independence of the internal audit function (refer to section 2.6.1 on p. 113).

- **Staff complement**

The literature highlights that the shortage of competent staff is a major concern for the internal audit profession (refer to section 2.6.3 on p. 119). Staff information varied considerable between the ten organisations, with between 12 to 328 full-time employees per organisation in the private sector, and 2 to 9 employees in the public sector. Table 5.4 on p. 319 summarises the average number of staff (*M*) for the internal audit function, as well as the average revenue (private sector) or average expenditure (public sector) covered per staff member for the

participating organisations. The reason for using the measurement of revenue or expenditure is explained under the heading 'Budget' on p. 321.

Table 5.4: Number of staff

	Private sector		Public sector	
	Mean (*M*)	**Revenue**	**Mean (*M*)**	**Expenditure**
Full-time employees	98.4		5.6	
Part-time employees	3.4		1	
Audit coverage per staff member	N/A	R718 million	N/A	R3 078 million

The above results indicate a significantly high number of average staff for the private sector. It should be noted that one private sector respondent is an international organisation with a group internal audit function situated in SA and internal auditors across the globe feeding into this function. Without taking this group into consideration, the remaining four participating organisations have an average of 41 staff members. With regard to the coverage of the revenue per internal auditor, on average, R718 million is covered per staff member (total revenue / number of internal audit staff). When comparing these figures to the IIA's benchmarking programme that incorporates information from participating private sector organisations across the globe (IIA 2007(b):9), the Global Audit Information Network (GAIN), similarly sized private sector organisations have, on average, a staff complement of 23 internal auditors. This comparison indicates that SA organisations are far better staffed, with an average of 98.4 staff members. Note that no other variables except the size of the organisation per revenue are taken into account when comparing this information to the GAIN programme. This tendency is confirmed with statistics on the revenue per internal auditor at $324 743 417 X R7 per $1 = R2 273 million (IIA 2007(b):13) compared to the R718 million for the participating SA organisations.

For the public sector, the internal audit function staff complement of the participating organisations is currently extremely low, with, on average, only 5.6 full-time employees and 1 part-time employee. Furthermore, on average, R3 078 million is covered per staff member to provide assurance on the expenditure of

the organisation. No comparative international benchmarking figures could be identified for the public sector.

- **Competencies of staff**

With regard to the competencies of the full-time internal audit staff (refer to sections 1.2.3 on p. 8, 2.6.3 on p. 119 and 2.7 on p. 130), information was gathered on their knowledge and skills, namely their professional qualifications, tertiary academic qualifications and internal audit experience. Table 5.5 below provides the results per sector. Note that for the private sector only 4 results are included due to the fact that one organisation's database did not have the relevant information for their internal auditors.

Table 5.5: Competencies of internal auditors

Qualification/Experience	Private sector		Public sector	
	Mean (*M*)	**% of full-time**	**Mean (*M*)**	**% of full-time**
Professional qualifications				
CA(SA)	10.75	26.2%	0.2	3.6%
CIA	6.5	15.6%	1	17.9%
CISA	7.25	17.7%	0.2	3.6%
Other	1.75	4.3%	0	0
Tertiary qualifications				
Doctorate/Masters degree	4.25	10.4%	0	0
Honours/B Tech	14.75	36%	1	17.9%
Degree/Diploma	15.5	37.8%	4.2	75%
Internal audit experience				
>10 years' experience	4.5	11%	1	17.9%
5-10 years' experience	11	26.5%	2.8	50%
2-4 years' experience	11	26.5%	1.6	28.6%
<2 years' experience	14.75	36%	0.2	3.5%

Note: For professional and tertiary qualifications the percentages do not add up to 100% as individuals could have more than one professional qualification, or no tertiary qualifications

For the private sector, 26.2% and 15.6% of internal auditors hold respectively either a CA(SA) and/or a CIA designation, the most recognised qualifications for SA professional internal auditors. These statistics are on par with the average for

CIAs in SA of 16.1% (refer to table 1 on p. 7). The percentage of internal auditors with the Certified Information Systems Auditor (CISA) qualification is also very high, even higher than the CIA qualification, with 17.7% and is in line with the need for professional IT auditors (refer to section 2.6.6 on p.126). With regard to tertiary qualifications, 84.2% of internal auditing staff hold some form of qualification. However, with regard to internal audit experience, only 37.5% of the staff have over five years of experience. This finding is in line with the discussion on the lack of competent internal auditors and shortage of skills (refer to sections 1.2.3 on p. 8, 2.6.3 on p. 119 and 2.7 on p. 130).

The public sector has 3.6% and 17.9% of their internal auditors holding a CA(SA) and/or a CIA designation respectively. This is above the average of 16.1% for SA internal auditors holding a CIA designation (refer to table 1 on p. 7). With regard to tertiary qualifications, the public sector has 92.9% of internal auditors holding a degree/diploma or honours degree/BTech. Furthermore, public sector internal auditors have higher levels of experience in internal auditing with 67.9% having more than five years' experience

- **Consultants**

The use of consultants by private sector and public sector in-house functions (note that this does not refer to outsourcing but the use of either individuals within the organisations or external experts that assist the in-house internal audit function) varies from 'never' to 'when required'. It is interesting to note though that consultants are never used for assurance or consulting activities with regard to the risk management framework and risk management process. This is contradictory to the discussion on the lack of internal auditors in certain specialisation fields, including risk management, as discussed in section 2.4.3 on p. 79.

- **Budget**

An effective and efficient internal audit function needs a sufficient budget (refer to section 2.7 on p. 130 and table 2.5 on p. 99). Although many other criteria could

be used to measure the internal audit function against, a common criteria is to use revenue (IIA 2007(b):7). However, for public sector organisations that do not have revenue, expenditure is more appropriate as their success is measured against the expenses incurred to reach their objectives. With regard to the internal audit function's comprehensive budget in terms of the organisation's financial activities and the external audit fees, table 5.6 below summarises the averages.

Table 5.6: Internal audit function's budget

	Private sector Mean (*M*)	**Public sector Mean (*M*)**
Budget in terms of revenue	0.28	N/A
Budget in terms of expenditure	N/A	0.17
Budget in terms of external audit fees	101.79	123.32

The average internal audit budget in terms of the organisations' revenue (private sector) and expenditure (public sector) is respectively 0.28% and 0.17%, both much higher than the benchmark according to the IIA's GAIN study for private sector organisations – 0.04% (IIA 2007(b):9). No benchmark information could be obtained for the public sector.

With regard to the internal audit budget as a percentage of the external audit fees, both the sectors exceed the norm of 70% (GAIN 2007(b):9), with the public sector internal audit budget being 123.32% of the external audit fees and 101.79% for the private sector. Again, no benchmark information could be obtained for the public sector.

- **Internal audit reporting lines**

As discussed in section 2.6.1 on p. 113, the reporting lines of the chief audit executive have a direct influence on the independence of the function, which in turn provides a platform for the standing of the function within the organisation as well as how other role-players perceive the function (refer to section 2.5.3 on p. 106). In table 5.7 on p. 323 shows the results for the reporting lines.

Table 5.7: Reporting lines of the chief audit executive

Position	Private sector		Public sector	
	Functional	Administrative	Functional	Administrative
Chief executive officer/Director general	0	1	0	5
Chief financial officer	0	3	0	0
Chair of the audit committee	5	N/A	5	N/A
Other	0	1	0	0

The above results correlate directly with the studies performed globally (refer to section 2.6.1 on p. 113). According to the literature and the results of this study, the reporting structures of the private sector vary, and many chief audit executives report administratively to the chief financial officer, increasing the possibility of jeopardising the function's independence.

The reporting structures of the public sector are in line with guidance and the literature, namely functionally to the audit committee chair and administratively to the director general, most probably due to this sector functioning in a strict legislative environment.

5.3.4.1.2 Existence and structures of various risk-related parties

- **Structures supporting risk**

As discussed in section 3.3.6.1 on p. 177 and identified in table 3.2 on p. 166, the risk committee (or in the absence of a risk committee, the audit committee) must assist the board with the execution of their responsibilities regarding the management of risks. Furthermore, as discussed in section 3.3.6.2 on p. 179 and identified in table 3.2 on p. 166, senior management should implement a risk department, or at minimum, employ a chief risk officer. In table 5.8 on p. 324, the results of the adherence to this guidance by participating organisations are summarised.

Table 5.8: Existence of an audit and/or risk committee and other risk structures

Structure	Private sector	Public sector
Board audit committee	2	2
Board risk committee	2	0
Board combined audit and risk committee	3	3
Risk department	5	1
Chief risk officer	5	4
Internal risk committee	2	3

For the private sector, the above results indicate that all of the organisations have established either an audit committee with a separate risk committee (two respondents), or a combined audit and risk committee (three respondents). With regard to the risk structures within the organisation, these organisations have a risk department with a chief risk officer heading the department, and a further two respondents indicated that their organisations have an internal risk steering committee.

For the public sector organisations, three respondents have a combined audit and risk committee whereas the other two only have an audit committee in place. The risk structures are still in a developing phase with only one organisation that has a risk department. The fact that executive management is still testing the ideal structure was confirmed by all of the public sector interviewees. Three participating organisations have an internal risk steering committee in place.

With regard to the board risk committee, the third King Report (2009:75) stipulates that in the absence of a risk committee, the audit committee should fulfil this role. However, the second King Report (2002:76) suggests that this arrangement is not recommended and should only apply due to economic reasons or another reason that is explained in the annual report, such as the lack of knowledgeable individuals. The third King Report (2009:75) also argues that this should be done with careful consideration. The management of risk needs individuals with operational and business knowledge such as executive directors and members of senior management with relevant skills. The audit committee should, however, be independent from the organisation's management and

needs individuals that are non-executive and independent (Marx 2008:363-364). Therefore, in an ideal situation these two committees should complement one another when it comes to risk management with the risk committee overseeing the management of risk and the audit committee overseeing the assurance thereof. The establishment of an internal risk committee could, however, be used to complement the audit committee's risk knowledge and expertise.

- **Composition of board committee(s)**

The structuring of the audit and/or risk committee(s) is of the utmost importance to ensure that risk is managed effectively. According to the third King Report (2009:57,75), the audit committee should comprise at least three members, all of whom should be independent and non-executive, and the risk committee should have a minimum of three members, including both executive and non-executive directors. The requirements of the PFMA will not be taken into account as it was promulgated in 1999 and the third King Report is also applicable for public sector organisations. The average numbers of committee members for the participating organisations are summarised in table 5.9 below.

Table 5.9: Composition of the audit and/or risk committees

Average members	Private sector		Public sector	
	Audit committee (incl. A&RC)	Risk committee (*)	Audit committee (incl. A&RC)	Risk committee (**)
Number of members	5.2	9.5	3.2	0
Executive/non-independent		3		0
Non-executive	0.6	1	0.6	0
Independent non-executive	4.6	5.5	2.6	0

A&RC – Audit and risk committee

(*) – 2 respondents

(**) – No respondents

The private sector participating organisations are in line with the King Report requirements with regard to the audit committee composition (4.6 members > 3 members should be independent non-executives). Although only two participating

organisations have separate risk committees, it is concluded that a variety of executive and non-executive members are serving on these committees, which is in line with the King Report requirements. The study performed by Marx (2008:363) on the audit committee composition of the top forty companies in SA confirms this tendency with an average of 4.15 audit committee members with an average of 3.4 being independent and non-executive. However, as listed in table 5.8 on p. 324 and discussed thereafter, three organisations do not have a separate risk committee and this could jeopardise the effective management of risks within these organisations.

The public sector participating organisations' audit committee members do not adhere to the King Report's guidance with an average of only 2.6 members being independent and non-executive. The fact that not one of these organisations has a separate risk committee and only three have a combined audit and risk committee means that the audit committees' activities are weakened even further.

- **Risk reporting lines**

The mere existence of a risk department and/or chief risk officer will not ensure the effective management of risk. Although not much formal guidance exists on the structure, responsibilities, duties and composition of these parties, the importance of their existence to management could perhaps be measured by their reporting lines – the more senior the reporting structures, the more probable that management views these as important bodies to manage risk (refer to section 3.3.6.2 on p. 179). In table 5.10 on p. 327 the participating organisations' reporting lines for their current risk structures are provided.

The results of the study confirm the thought that risk management structure is a new concept and that the board and senior management may still be unsure as to where to position it in the organisational structure. It is, however, reassuring that all the respondents that indicated that their organisations have a risk department and/or chief risk officer indicated that their risk structures report to the board and/or director level.

Table 5.10: Reporting lines of risk structures

Position	Private sector		Public sector (*)	
	Risk department	Chief risk officer	Risk department	Chief risk officer
Board risk or audit & risk committee	4	0	1	2(**)
Chief executive officer/Director general	0	2	0	2(**)
Risk director	1	0	0	0
Chief financial officer	0	1	0	0
Governance director	0	2	0	0
Director corporate services	0	0	0	1
Chief operating officer	0	0	0	1
TOTAL (refer to table 5.8)	5	5	1	4

(*) – 4 respondents

(**) – The chief risk officer has dual reporting lines for two organisations

For the private sector, the majority of the risk departments in the study report to a board committee, but chief risk officers have to report to various managerial positions. All the organisations do have a risk department as well as a chief risk officer (refer to table 5.8 on p. 324).

With regard to the public sector, no separate risk committees exist (refer to table 5.8 on p. 324) for the responding organisations in this study. Two of the participating organisations' chief risk officers report to the combined audit and risk committee as well as the director general. The third organisation has a separate risk department that reports to the combined audit and risk committee and the chief risk officer reports to the chief operating officer. The fourth organisation's chief risk officer also reports to the director level.

5.3.4.1.3 Coordination of risk-related activities

- **Internal auditing and risk structure**

In section 3.3.6.2 on p. 179, the role and responsibility of the internal risk management function(s) are discussed. The coordination of the internal audit

function with the risk department and/or the chief risk officer as well as the internal risk committee will ensure that all the activities related to risk are covered. Furthermore, when new or crucial risks are exposed by either internal auditing or risk management, this should be made known to the other party. This will ensure that risks are managed in a timely, effective and efficient manner. As discussed in section 4.3.2.1.1 on p. 243, internal auditing is responsible for mapping all of the assurance activities of the organisation, including the assurance provided by the risk management structure. Suitable coordination will enhance this responsibility. In table 5.11 below a few of these coordinating activities are summarised.

Table 5.11: Coordination between the internal audit function and the internal risk structures

	Private sector	Public sector (*)
Report relevant information to each other	2	2
Regular informative meetings	3	3
Copy each other on reports	4	2
Assist each other with duties	1	3

(*) – 4 respondents

Although the results indicate that the most common form of coordination in the private sector is the copying of reports to the other party, it is reassuring to note that regular informative meetings occur at the participating organisations.

In line with the other results that indicate that risk management in the public sector is still a new concept, the internal audit function and risk structures assist one another with their duties. For example, the respondents indicated that internal auditing assist with the establishment of risk structures and models and facilitate risk workshops. Most of the respondents in the public sector indicated that until recently internal auditing was responsible for the risk management activities; therefore, it is fair to assume that internal auditing most probably assist the risk structures more often than the other way around. Other comments include that internal auditing has a standing invitation to the internal risk steering committee, serves in an advisory position, or even has a permanent position on this committee, as well as both internal auditing and risk management serving on a combined assurance forum.

- **Audit committee and risk committee**

Both the audit committee and the risk committee are board committees. It appears that the trend may be to have these two committees combined as one board committee, namely the audit and risk committee (refer to table 5.8 on p. 324). However, as debated on p. 324, it is advisable to have separate committees. In the cases where two different committees exist, the coordination between these committees is as summarised below in table 5.12.

Table 5.12: Coordination between the audit committee and the risk committee

	Private sector(*)	Public sector(**)
Members serve on the other committee	2	0
Read minutes of each other's meetings	0	0
Specific report to each other	0	0
Assist each other with duties	0	0

(*) – 2 respondents

(**) – No respondents

From the information in table 5.8 on p. 324, the existence of a separate risk committee is still very limited, with only two of the ten participating organisations having a separate board risk committee. Effective communication is very important for sound governance in any organisation, including the communication between the risk committee and the audit committee as overseers of the risk management framework. However, at both of the organisations in the private sector with separate board risk and audit committees, the internal audit functions, apart from being aware that members from these two committees serve on the other committee, were unsure of the coordination between the risk and the audit committees. Being that only two separate risk committees were reported and that internal auditing was unsure as to the coordination between the various bodies, this area needs further improvement.

- **Internal auditing and risk committee**

Although the internal audit function should report to the risk committee *via* the audit committee, it could be possible that direct coordination exists between internal auditing and the risk committee. According to guidance (refer to table 3.2 on p. 166) this coordination should at least include the reporting of the assurance provided by internal auditing on risk management. In table 5.13 below, the coordination between the internal audit function and the risk committee for the responding organisations is summarised. Where the risk committee is part of the audit committee, the coordination with this committee is also indicated.

Table 5.13: Coordination between the internal audit function and the risk committee/audit and risk committee

	Private sector		**Public sector**	
	Risk committee (*)	**Audit & risk committee (**)**	**Risk committee (***)**	**Audit & risk committee (****)**
IAF reports to risk committee on relevant findings on risk management	1	3	0	0
IAF provides risk committee with assurance regarding risk concepts	1	3	0	1
Risk committee asks IAF for input regarding risk concepts	0	1	0	1
IAF reports to risk committee on risk management responsibilities	1	2	0	0

IAF – Internal audit function

Refer to table 5.8 on p. 324 for the existence of these committees:

(*) – 2 respondents *(**) – 3 respondents*

(***) – No respondents *(****) – 4 respondents*

The results indicate that there is coordination between the internal audit function and the risk (or audit and risk) committee. For the private sector, the results correlate with what is expected of internal auditing, namely providing assurance services (refer to the first two areas in table 5.13 above). Other coordination

includes internal auditing reporting to the committee on the annual risk management framework and internal auditing having an open invitation to submit reports as deemed necessary. An area that still needs to be explored in greater depth is the risk committee asking for the input of internal auditing regarding risk concepts.

For the public sector respondents, coordination is very limited with internal auditing mostly reporting on aspects discovered while performing audit engagements that could affect risk management.

5.3.4.1.4 Adherence to the IIA *Standards*

- **General adherence**

As discussed in section 1.2.4.7 on p. 11, studies indicate that not all internal audit functions adhere to the IIA *Standards.* To determine whether this study's respondents adhere to the *Standards* with regard to the management of risk, it was first necessary to determine whether they adhere to the *Standards* in general. Four of both the private sector respondents as well as the public sector respondents indicated that they always adhere to the *Standards*. The remaining one respondent in each of the two sectors indicated that they have not performed a quality assessment as required by the *Standards*, and thus do not fully adhere to the *Standards*. This is in line with the tendency identified in the CBOK study as discussed in section 1.2.4.7 on p. 11.

- **Risk management**

In section 4.3.1.2 on p. 239, the role of internal auditing with regard to risk management is discussed. Although not much information is available on the assurance that internal auditing provides on the overall risk management framework, areas of research refer to the assurance on the risk management process and whether risks are evaluated correctly, which is in line with the *Standards*. Table 5.14 on p. 332 gives the results for adherence to the applicable

standards that reflect on risk management. The table also indicates if the study's respondents believed that more guidance is needed to adhere to a specific standard, and for the public sector (due to low risk maturity) when the implementation of the applicable standards would occur (if they are not currently adhered to).

Table 5.14: Adherence to standards related to risk management activities

Activity	Private sector				Public sector					
	Adherence		Guidance		Adherence		Guidance		Implementation	
	Yes	No	Yes	No	Yes	No	Yes	No	In 1 year	In 2-3 years
IAF evaluates the effectiveness of risk management (Standard 2120)	5	0	0	5	1	4	2	3	2	2
IAF contributes to the improvement of risk management (Standard 2120)	5	0	0	5	1	4	2	3	2	2
IAF evaluates the risk exposure of the organisation (Standard 2120.A1)	4	1	0	5	1	4	2	3	2	2

IAF – Internal audit function

Only one private sector organisation respondent indicated that they do not fully adhere to the internal audit function evaluating the risk exposure of the organisation, the reason being that certain activities are too technical and actuaries are needed to perform this task. According to Standard 1210.A1 (IIA 2009(a):18-19) this is not a valid excuse as internal auditing should contract experts when such knowledge is lacking within the internal audit function.

For the public sector, only one participating organisation adheres to the above standards with reasons for non-adherence ranging from the fact that the organisation does not have a risk management framework in place, to the risk

department being a new function and not yet fully operative. All the respondents indicated that adherence will be implemented within one (two organisations) to between two to three years (two organisations). Lastly, it is noted that some public sector organisations require further guidance on how to perform these tasks.

- **Internal audit function's annual plan**

In section 4.3.2.2 on p. 244, it is concluded that most organisations do adhere to the IIA *Standards* related to the setting of the internal audit function's annual plan. However, the literature studies mentioned in this section do not include the possibility of the internal audit function performing consulting activities to improve the risk management framework. In table 5.15 on p. 334 adherence levels to the *Standards* that refer to the planning of the internal audit function's activities linked to risk are summarised. The summary includes whether further guidance is needed by respondents and when implementation could be expected (if applicable) for the public sector.

It is concluded that the overall results are in line with the literature as discussed above – the participating organisations have a risk-based annual plan in place as drawn up by the internal audit function, but the function does not perform consulting services to improve risk management.

The private sector organisations' respondents suggested that more guidance is needed to perform these tasks. Reasons for non-adherence to the consulting activities range from the fact that the internal audit function only perform assurance services, the function does not have enough employees and/or expertise, and the risk department is providing sufficient improvement to the risk management framework.

Table 5.15: Adherence to standards related to planning the internal audit function's annual activities

Activity	Private sector				Public sector				
	Adherence		Guidance		Adherence		Guidance		Implementation
	Yes	No	Yes	No	Yes	No	Yes	No	Never
The IAF's annual plan is risk-based, after performing an assessment (Standards 2010 & 2010.A1)	5	0	1	4	5	0	0	5	N/A
The IAF accepts consulting engage-ments to improve risk management (Standard 2010.C1)	2	3	2	3	4	1	0	5	1

IAF – Internal audit function

The private sector respondents suggest that more guidance is needed to perform these tasks. Reasons for non-adherence to the consulting activities range from the fact that the internal audit function only perform assurance services, the function does not have enough employees and/or expertise, and the risk department is providing sufficient improvement to the risk management framework.

The public sector respondents did not express a need for further guidance. Respondents indicated that the risk structure of the organisation is capable in providing this service, but, where needed, the internal audit function will accept consulting engagements to assist the risk structure in improving risk management.

- **Risk-based audit engagements**

In section 4.3.3.2 on p. 249, the implications of a risk-based approach when conducting internal audit engagements are debated. Although it was found that information is limited, this remains one of the areas that will have to receive more

attention in the future in order to improve internal auditing's risk-related competencies and mindset as well as enabling the function to be more effective and efficient in adding value to the organisation. The results of adherence of the participating organisations to the related standards, whether more guidance is needed, and the expected implementation date (if applicable) for public sector organisations (due to their low risk maturity levels) are summarised in table 5.16 below.

Table 5.16: Adherence to standards related to the performance of risk-based internal auditing engagements

Activity	Private sector				Public sector					
	Adherence		Guidance		Adherence		Guidance		Implementation	
	Yes	No	Yes	No	Yes	No	Yes	No	Never	In 2-3 years
Consider the significant risks (Standard 2201)	5	0	1	4	5	0	0	5	N/A	N/A
Consider how risk is kept to acceptable levels (Standard 2201)	5	0	1	4	5	0	0	5	N/A	N/A
Consider adequacy of relevant risk management process (Standard 2201)	5	0	1	4	4	1	0	5	0	1
Consider effectiveness of relevant risk management process (Standard 2201)	5	0	1	4	4	1	0	5	0	1
Perform risk assessment to determine engagement's objectives (Standard 2210.A1)	4	1	1	4	4	1	0	5	1	0

For the private sector, the respondents were of the view that risk-based internal audit engagements are performed, with only one organisation confirming that no

risk assessment is performed. The respondents' risk departments perform this task and their internal audit functions use the outcome of this process to determine their engagement objectives. One respondent indicated that further guidance is needed on this topic apart from the guidance in the *Standards* and practice advisories.

Apart from one participating public sector respondent indicating that no risk management process exists within the organisation, the rest of the respondents were of the view that risk-based internal audit engagements are performed. One respondent indicated that the internal audit functions do not perform a risk assessment as this task is performed by the risk department.

5.3.4.1.5 Internal auditing's involvement in risk management

- **Areas of involvement**

This section investigates the risk management activities that internal auditing could undertake. Although guidance is specific on what internal auditing's involvement should be, this is not necessarily the view of management and the board, and could affect the practical implementation of the risk-related activities (refer to section 4.3.1.2 on p. 239). In table 5.17 below, the respondents' points of view regarding the areas of involvement expected of the internal audit function, as guided by the IIA *Standards* and practice advisories, are given.

Table 5.17: Viewpoint on the areas of involvement in risk management

	Private sector	Public sector
Provide assurance on the risk management framework	5	5
Provide assurance on the risk management process	5	5
Participate in consulting activities	5	2
Take full/partial responsibility for implementing the risk management framework	0	0
Taking full/partial responsibility for implementing the risk management process	0	0

The private sector respondents' internal audit functions include the first three areas but the interviewees indicated that internal auditing can only provide input in the risk management framework and/or process as it remains management's responsibility to implement these structures. Concerns were raised that the internal audit function lacked resources to provide consulting activities, and should be cautious when accepting such engagements.

With regard to public sector organisations, all the respondents agree that assurance activities should be performed but only two agree with internal auditing also performing consulting activities. The reasons provided include that consulting activities should be performed by the risk department and internal auditing should remain independent.

- **Increased involvement**

The involvement of internal auditing in risk management has most probably increased over the last decade due to increased corporate governance legislation and guidance. Below, in table 5.18, the respondents' viewpoints on whether internal auditing's involvement in risk management has increased over the last decade (1999 and onwards) are summarised.

Table 5.18: Viewpoint on the increased involvement in risk management

	Private sector	Public sector
Last 6 months	0	0
Last year	1	2
Last 3 years	1	1
Since PFMA	N/A	0
Since second King Report (King II)	3	2
Since third King Report (King III)	0	0

For the private sector participating organisations, internal auditing's increased involvement in risk management activities occurred mainly due to the issuing of the second King Report (IOD 2002). Comments include the fact that internal auditing had to appoint specialists to perform certain duties, that internal auditing had first developed risk management for the organisation but since King II the

function now has an assurance role to play, that internal auditing was assisting with the implementation of a risk department, and that internal auditing recently starting to develop their annual internal audit plan based on a risk assessment.

The public sector participating organisations risk management involvement has also mainly increased due to the issuing of the second King Report in 2002, or, over the last year, due to the implementation of a risk management framework, for example, a chief risk officer has been appointed. However, not one participating respondent indicated that the PFMA has influenced the internal audit function's increased involvement, even with the PFMA (SA – 1999:S38(1)) enforcing that a risk assessment should be conducted and that internal auditing should use the outcome to guide their activities.

- **Future increase in involvement**

The future involvement of internal auditing could be affected by certain current factors such as the current global financial crisis and the new guidance issued, to name but a few (refer to sections 2.4 on p. 70, 2.5 on p. 84 and 2.6 on p. 113). Table 5.19 below gives the viewpoints of the respondents regarding the factors affecting the potential future increase of internal auditing's involvement in risk management.

Table 5.19: Viewpoint on the future increased involvement in risk management

	Private sector	Public sector
King III guidance	4	4
Current financial crisis	0	0
Board's/Executive's changed needs	2	2
Management's changed needs	1	3

Most of the respondents at the private sector organisations were adamant that internal auditing's involvement should not increase as this could jeopardise the function's independence. However, they felt more emphasis could be placed on the current risk management activities performed mainly due to the issuing of the

third King Report (IOD 2009) and the board of director's changed needs (one respondent also mentioned the new Companies Act as a reason). One area that most probably would be added to internal auditing's duties is combined assurance mapping (refer to section 4.3.2.1.1 on p. 243). It is noted that no respondents were of the view that the current financial crisis will have an influence on the increased involvement of the internal audit function in risk management. This is most probably due to the fact that most perceive this crisis to have an effect on the global market and are unaware of how this crisis has and will affect the SA market (Van Zyl 2010:1).

With regard to the public sector organisations' respondents, future involvement was also linked to, apart from the issued third King Report (IOD 2009), management's changed needs. This is mostly attributed to the fact that the risk structures are fairly new and internal auditing's role with regard to risk management is now entering a new dimension.

- **Factors affecting involvement (public sector)**

As all the organisations in the public sector were risk immature according to the first empirical study (refer to section Annexure H on p. 479), it is important to understand which factors could influence the role of internal auditing in risk management and to understand whether these could be altered, or whether internal auditing could provide management with guidance. In table 5.20 on p. 340 the viewpoints of the respondents are summarised with reference to the factor having no, a moderate or an extreme effect within their specific organisation.

Table 5.20: Factors influencing the public sector's involvement in risk management

Factor	No effect	Moderate effect	Extreme effect
The growth in corporate governance guidance, specifically with regard to risk management	0	0	5
The growth in corporate governance legislation, specifically with regard to risk management	0	2	3
The complexity of the international environment (e.g., globalisation)	2	1	2
The continual occurrence of financial scandals in the public sector	0	4	1
The current global financial crisis, owing to the perception that risk management was not properly introduced	1	2	2
The public's increased demand for accountability	0	1	4
The IAF's status within the organisation	1	1	3
The IAF's reputation within the organisation	1	0	4
Internal auditing having an overall understanding of the organisation's environment	0	1	4
Management perceive internal auditors to be control experts	0	2	3
Management perceive internal auditors to be risk experts	0	3	2
Other: No implementation of a risk structure (chief risk officer and risk department)			1
Other: New director general appointed that has a greater understanding of risk management			1

IAF – Internal audit function

It appears that the factor that has the most effect on a public sector internal audit function's involvement in risk management is the increased corporate governance guidance on risk management. This is in line with the results as indicated in tables 5.18 on p. 337 and 5.19 on p. 338. Other factors that have an extreme effect include the public's increased demand for accountability (refer to sections 2.3 on p. 63 and 3.2.4 on p. 150), the internal audit function having a sound reputation within the organisation (refer to section 2.7 on p. 130) and internal auditing having an overall understanding of the organisation's environment. Factors having a moderate to extreme effect include the increase in corporate governance legislation and guidance on risk management (refer to section 3.3.4

on p. 163), the occurrence of financial scandals (refer to section 3.2.3.1 on p. 146), and management perceiving internal auditors to be both risk and control experts.

5.3.4.1.6 Internal audit activities related to the risk management framework

- **Current and future activities**

Although the IIA's position paper (IIA 2004) provides guidance to the internal audit function on what its role should be with regard to the risk management framework, the management of organisations sometimes has other opinions as to what this should entail (refer to section 4.3.1.2 on p. 239). In table 5.21 on p. 342, the participating organisations' activities that are currently performed as well as planned activities are listed in terms of core or desirable activities, activities that could be performed but with caution, and activities that should be avoided at all costs (refer to figure 4.1 on p. 237). Note that the activities are summarised as either consulting and/or assurance activities as this could influence whether a certain activity performed is in line with guidance or whether it is against good practices (refer to section 2.4.1.1 on p. 71).

It is reassuring to note that the roles that internal auditing should not undertake according to the guidance are not being performed by both sector's internal audit functions.

For the private sector, the participating internal audit functions are currently providing assurance on the core activities and although performing some of the additional legitimate internal audit roles, are planning to minimise these in the future.

Table 5.21: Current and future activities related to the risk management framework (consulting *versus* assurance activities)

Activity	Current activity				Future activity			
	Consulting		Assurance		Consulting		Assurance	
	PR	PU	PR	PU	PR	PU	PR	PU
Core Activities								
Providing assurance on the effectiveness of the risk management framework	0	0	5	1	0	1	5	5
Evaluating the methodology of the risk management process(es)	1	0	5	1	1	1	5	5
Evaluating the reporting of key risks	0	1	5	3	0	0	5	5
Reviewing the management of key risks	0	1	5	3	0	0	5	5
Legitimate internal audit roles with safeguards								
Facilitating the identification and assessment of risks	1	3	2	0	0	1	2	0
Coaching management in responding to risks	1	4	1	0	0	1	1	2
Coordinating organisation-wide risk management activities	0	3	0	0	0	1	0	0
Developing the risk management framework	0	3	1	0	0	1	1	0
Maintaining the risk management framework	0	3	1	0	0	1	1	0
Roles internal auditing should not undertake								
Setting the risk appetite	0	0	0	0	0	0	0	0
Taking part in the risk management process(es)	0	0	0	0	0	0	0	0
Taking decisions on risk responses	0	0	0	0	0	0	0	0
Implementing risk responses	0	0	0	0	0	0	0	0
Being accountable for risk management	0	0	0	0	0	0	0	0

PR – Private sector

PU – Public sector

Public sector organisations are performing more consulting activities, probably due to the fact that risk management is relatively new in the public sector and internal auditing is assisting management to get the risk management framework

in place. This is, however, not in line with the viewpoint of chief audit executives (refer to table 5.17 on p. 336). According to the IIA's guidance, this is acceptable as long as internal auditing implements safeguards to ensure that their independence is not compromised. Lastly, it is concluded that all the participating organisations are currently performing, or are planning to provide assurance services on core activities.

- **Factors preventing public sector involvement**

As discussed in section 5.2.3 on p. 304, the public sector is lacking risk maturity. Table 5.22 below summarises the respondents' viewpoints on which factors could hinder the internal audit function's involvement in the risk management framework. This could provide public sector chief audit executives with insight into which areas they need to address to improve risk maturity within their organisations.

Table 5.22: Factors hindering the public sector's involvement in the risk management framework

Factor	No	Limited	Yes	N/A
IAF's lack of knowledge of the organisation	5	0	0	0
Internal auditor's lack of general risk knowledge	4	1	0	0
Limited skills of the internal audit staff complement	3	2	0	0
Limited competencies of the audit staff complement	3	2	0	0
Limited available tools (e.g., IT software) to assist internal auditing	1	2	2	0
Limited resources available to the IAF	0	2	3	0
Expectations of management of IAF duties to be performed too broad	2	1	2	0
Internal auditing has no/limited access to senior management	5	0	0	0
Internal auditing has no/limited access to the audit committee	5	0	0	0
Internal auditing has no/limited access to the risk department	1	0	0	4
Internal auditing has no/limited access to the chief risk officer	4	0	0	1
Internal auditing has no/limited access to the risk committee	0	0	0	5
The overall risk management strategy is ineffective	3	1	1	0
The organisation has a low risk maturity	2	2	1	0
Other: No implementation of a risk structure (chief risk officer and risk department)			1	

The results indicate the factor that hinders the internal audit function the most in performing services to the organisation regarding risk management is the limitation of resources, with the limited tools availability and management expecting too much of internal auditing tied in second place. In organisations where the risk management framework is partiality or fully implemented, internal auditing has full cooperation with the various risk parties and access to all relevant material and information.

5.3.4.1.7 Internal audit activities related to the risk management process

- **Risk management process and risk register**

The risk management process (refer to section 3.5 on p. 191) and the role of internal auditing in this process (refer to section 4.5 on p. 258) are discussed in detail in the literature study. It was also concluded that the outcome of the risk management process can be used by the internal auditor to perform a risk-based internal audit engagement. The implementation of the process on various levels within the organisations (refer to sections 3.7.1.2 on p. 217 and 4.5.3.3 on p. 267) as well as the documentation of the outcome of the process in a risk register (refer to sections 3.5.3 on p. 203 and 4.5.3.2 on p. 266) are two important elements that need to be in place in order for internal auditing to use the outcome of the process. In table 5.23 below the implementation of the various elements of an effective risk management process by the participating organisations is summarised.

Table 5.23: The level of implementing a risk management process(es) and the implementation of a risk register

Organisational level	Private sector		Public sector	
	Process	Risk register	Process	Risk register
Strategic	5	5	4	4
Operational	5	5	4	4
Organisation-wide	2	2	1	1

With regard to the private sector participating organisations, all of them have implemented risk management processes on the strategic and operational levels. However, only two have implemented an integrated organisation-wide risk management process. The outcome of all the processes is documented in a risk register. Programmes used by the private sector include Microsoft Excel spreadsheets, an in-house programme developed by the organisations, Cura Software Solutions and MethodWare.

Only one participating public sector organisation has not yet implemented a risk management process. At the same time, only one participating organisation has implemented an integrated organisation-wide risk management process. The outcome of all processes is documented in a risk register and programmes used include Microsoft Excel spreadsheets, BarnOwl and Hummingbird.

- **Responsible party**

According to table 5.8 on p. 324, with the exception of one public sector organisation, most of the participating organisations do have a risk management structure in place that should be responsible for the implementation of the risk management process (refer to sections 3.3.6.1 on p. 177 and 3.3.6.2 on p. 179). In table 5.24 below the responsible parties for the various organisational levels of risk management processes are summarised.

Table 5.24: Parties responsible for the risk management process(es) on various organisational levels

Level of organi-sational process	Chief risk officer		Risk department	
	Private sector	Public sector	Private sector	Public sector
Strategic	1	3	4	1
Operational	1	3	3	1
Organisation-wide	1	1	1	0

Compared to table 5.8 on p. 324, the private sector's participating organisations do have risk departments headed by a chief risk officer. In these organisations, the department mostly takes the responsibility for the implementation of the risk

management processes at various organisational levels (refer to table 5.23 on p. 344). One private sector organisation uses the internal risk steering committee for operational risk management processes.

For public sector organisations, only one participating organisation indicated (refer to table 5.8 on p. 324) that a risk department is in place, in which case this department takes responsibility for the risk management processes on all the implemented levels. In all the other participating organisations (refer to table 5.23 on p. 344) the chief risk officer takes responsibility for the implementation of the risk management processes on strategic and operational levels. For the one organisation that indicated that they perform organisation-wide risk management processes, the chief risk officer is responsible for the implementation and execution of these processes. It is questionable whether one person can take on such a huge task successfully.

- **Risk register update**

According to section 3.5.3 on p. 203, the risk register should be updated on a regular basis so that the emerging of new risks or a change in the measurement of an existing risk can be properly communicated to all relevant parties. The frequency of the updating of the risk register by participating organisations is summarised in table 5.25 below.

Table 5.25: Update of the risk register

Frequency	Private sector	Public sector
Continuously	2	0
Monthly	3	2
Bi-annually	0	0
Less frequent	0	0
Not known	0	2

For the private sector, most of the participating organisations update their risk register on a monthly basis, with the next most common method being a continuous updating process.

With regard to the public sector participating organisations, one has no risk register (refer to table 5.23 on p. 344) and two update their risk registers on a monthly basis. It is, however, concerning to note that for two of the public sector organisations, the chief audit executive was not sure as to the frequency of the update of the risk register.

- **Internal auditing's involvement**

In section 4.3.1 on p. 234, the role that internal auditing should play in the risk management process is discussed. Table 5.21 on p. 342, shows that all the participating private sector organisations indicated that the internal audit function are evaluating the risk management process methodology followed and are providing assurance thereon. Three participating organisations indicated that they are facilitating the identification and assessment of risks by performing either consulting activities or assurance activities.

With regard to the public sector, according to table 5.21 on p. 342 only one participating organisation is adhering to the guidance on evaluating the risk management process methodology, but all are planning to perform this task in future. Furthermore, three of the participating public sector organisations indicated that they are facilitating the identification and assessment of risks by performing consulting activities. In table 5.26 below the participating organisations' internal audit involvement in the risk management process is listed.

Table 5.26: The role of internal auditing in the risk management process

	Private sector	Public sector
Organisational risk register updated with results of internal audit engagements	5	4
No involvement in the process	0	3
Audit the effectiveness of the process methodology	5	1
Audit the results of the process	4	1
Facilitate the process	0	1
Take partial responsibility for the process	0	0
Take full responsibility for the process	0	0

Table 5.26 is divided into two sections; above the bold line, the results for the inclusion of internal audit engagement findings in the organisational risk register is indicated, and under the bold line, the role that internal auditing plays regarding the overall risk management process is provided.

All the participating organisations, in both the private and public sectors, that do have a risk register use, *inter alia*, the results of internal audit engagements to update the risk register.

For the private sector all internal audit functions audit the effectiveness of the methodology followed, which is in line with table 5.21 on p. 342, and audit the results of the process. However, regarding the facilitation of the process, in contrast to the results in table 5.21 on p. 342) internal auditing has no involvement.

For the public sector, three of the participating respondents indicated that internal auditing has no involvement in the risk management process, with one indicating that internal auditing evaluates the effectiveness of the process (in line with the results according to table 5.21 on p. 342)., and one assisting with the facilitation of the process (three according to table 5.21 on p. 342).

It appears that respondents in both the sectors could still be unsure as to which duties the internal audit function are actually performing, or, probably more accurately, are unsure as to how to describe the actions and duties being carried out.

A further concern is that three of the public sector organisations are performing no activities with regard to the risk management process.

5.3.4.2 Inclusion of risk concepts into the internal audit function's activities

In section 5.3.1.2 on p. 311, it is concluded that the literature proves that the first step for the internal audit function in incorporating risk-related aspects into their

activities is the planning of the internal audit functions' annual plan using a risk assessment. Although the actual planning is not included in the scope of this study, it is a vital clue as to whether respondents do view risk-related aspects as important.

- **Guidance**

Guidance exists for both the private and the public sectors' internal audit functions (refer to section 4.3.2 on p. 242) on how to establish the functions' annual plans. In table 5.27 below adherence to this guidance by the participating organisations is indicated, as well as when implementation will occur if an organisation has not yet implemented the guidance. King III guidance is used for both the sectors, with the PFMA being applicable to the public sector only.

Table 5.27: Adherence to guidance related to the risk-based planning of the internal audit function's annual plan

Activity	Private sector		Public sector			
	Adherence		Adherence		Implementation	
	Yes	No	Yes	No	Never	In 2-3 years
King III Guidance						
Plan based on a risk and opportunities assessment performed (key risk areas)	5	0	5	0	N/A	N/A
Plan based on risks identified by management	5	0	5	0	N/A	N/A
Plan based on opportunities identified by management	4	1(*)	3	2	1	1
Plan aligned with the results of the risk management process(es)	5	0	4	1	0	1
PFMA						
Current operations taken into account	N/A	N/A	5	0	N/A	N/A
Proposed operations in the organisation's strategic plan taken into account	N/A	N/A	5	0	N/A	N/A
Risk management strategy of the organisation taken into account	N/A	N/A	3	2	0	2

(*) – Implementation will never occur

For the private sector, all the participating organisations perform a risk assessment in order to develop the internal audit year-plan, which includes the identification of risks by management. However, one organisation does not include the identification of opportunities by management as part of the process and indicated that this will never occur.

Participating public sector internal audit functions perform risk assessments when developing their annual plan, including the identification of risks by management. Again, it is concluded that not all of the organisations base their plans on the opportunities identified by management or even align the plans with the results of the risk management process. Furthermore, it appears that two of the organisations are not adhering in full to the public sector legislation. This is a concerning fact as the PFMA was promulgated in 1999, more than ten years ago.

- **Factors preventing public sector adherence**

Only two public sector organisations indicated that they do not adhere fully to the above guidance (refer to table 5.27 on p. 349). In table 5.28 below, these two respondents provide possible factors hindering the internal audit function from adhering to the guidance.

Table 5.28: Factors hindering public sector internal auditing from adhering to guidance on planning the function's annual plan

Factor	No	Limited	Yes
Lack of executive commitment to risk management	2	0	0
Lack of executive commitment to internal auditing	2	0	0
Lack of management commitment to risk management	2	0	0
Lack of management commitment to internal auditing	2	0	0
The IAF has limited resources	0	0	2
The IAF has limited available tools (e.g., IT software)	0	1	1
The overall risk management strategy is ineffective	0	1	1
The organisation has a low risk maturity	1	0	1
Other: Lack of management knowledge of risk management		1	
Other: Risk management is a new activity			1

IAF – Internal audit function

As indicated in table 5.22 on p. 343, regarding the factors hindering the internal auditing functions' involvement in the risk management framework, the factor that again hinders internal auditing in their efforts to provide the most effective and efficient service as per the guidance is the lack of resources, including available tools. Respondents are further concerned that the overall risk management is ineffective. It is concerning to note that one of the respondents persists in believing that the low risk maturity of the organisation (refer to table 5.2 on p. 316 for the views of respondents on the risk maturity score) has no implications for its successful planning of the internal audit function's activities. Additional to the list provided, the two chief audit executives were also concerned about the lack of management's knowledge on the topic of risk management as well as the limited value of risk management to the annual internal audit function's planning activities due to a newly established risk management structure.

5.3.4.3 Risk-based planning of internal audit engagements

As discussed in section 5.3.1.3 on p. 312, only the private sector participated in this section of the questionnaire due to the low risk maturity of the public sector's participating organisations. The objectives of this section were to get an understanding of the methodology in place when planning an internal audit engagement, as well as whether the methodology followed could be used to implement the preliminary risk-based internal audit model as developed in section 4.5. on p.258. The study focuses on the planning phase of the engagement, as this is where the different methodologies are the most visible.

- **Methodology followed**

As discussed in section 4.5.4.2 on p.270 and analysed in table 4.5 on p. 272, most modern internal audit approaches can be linked to either the COSO I model (1992) or the COSO II model (2004). The study's respondents identified the approach they regard as relevant to their organisation (refer to table 5.29 on p. 352 – before). Thereafter, the application of the risk-based engagement models' methodology in an internal audit assurance engagement was explained to the

respondents after which they could re-evaluate their view of the current approach followed (refer to table 5.29 below – after).

Table 5.29: Methodology used during internal audit engagements

COSO I		COSO II		Other		Not sure	
Before	**After**	**Before**	**After**	**Before**	**After**	**Before**	**After**
2	3	2	1	1	1	0	0

The results indicate that the respondents can link their internal audit methodology used during engagements to either the COSO I model or the COSO II model, with only one respondent suggesting that their self-developed methodology is a combination of the two models. After the application of the models' methodology in an internal audit assurance engagement was explained to the respondents, one organisation came to the realisation that their methodology followed the first model more closely, instead of the second as initially perceived by the chief audit executive.

- **Starting point during planning**

As discussed in section 4.5.4.1 on p. 268 and analysed in table 4.4 on p. 269, the starting point of the planning of an engagement could vary depending on the methodology followed. Although both COSO I and II focus on the incorporation of risks into the internal audit engagement, the latter focuses on the difference between the inherent and residual risk ratings for each individual risk. In table 5.30 below the elements that are considered by the participating organisations when planning an engagement are summarised.

Table 5.30: The elements in use as the starting point of the planning phase

Previous year's working papers	Inherent risks as per the risk register	Difference between the inherent and residual risks as per the risk register
4	5(*)	4(*)

(*) – Refer to discussion below

The results indicate that the element that is incorporated into the planning phase of an internal audit engagement at all times is management's measurement of the

inherent risks documented in the participating organisations' risk registers. Two of the respondents indicated that, although they do consider the inherent risks as per the risk register as well as management's assessment of the inherent and residual risks (included in the above figures – refer to (*) in the above table), they rely more on the outcome of their own risk assessment. Therefore, it is assumed that the previous year's working papers are the most commonly used planning aid.

- **Information obtained**

Section 4.5.5 on p. 274 describes the preliminary risk-based internal audit engagement model developed by using the risk management process when performing the internal audit process. In table 4.6 on p. 275 the steps are analysed to determine how the various risk management process elements are treated in the planning phase of an internal audit engagement. The respondents' views on how the information is obtained regarding each key element of the risk management process that is used in the internal audit engagement are summarised in table 5.31 below.

Table 5.31: The information obtained on key elements of the risk-based internal audit engagement planning phase

Key elements	Use auditee input	Use risk management process results (risk register)	No/limited information (internal auditor has to obtain)
Operational (auditee) objective setting	4	5	4
Risk identification for inherent risks	2	5	2
Risk assessment (measure) for inherent risks	1	5	2
Current risk mitigation activities	2	3	5
Risk assessment (measure) for residual risks	0	4	3

The results indicate that most of the respondents use the risk register to obtain the auditee's objectives, inherent risks and their assessment, with additional gathering of information by either obtaining the auditees' input or the internal auditor performing certain tasks. This is in line with the results provided in table

5.30 on p. 352 on the inherent risks and the two respondents indicating that they also perform their own assessment.

It appears that internal auditing prefer to rely on their own interpretation of the current mitigation activities that are in place, with all five respondents indicating that internal auditors obtain this information with limited input from the auditees (two respondents) and the risk register (three respondents). However, in contrast to this fact, respondents indicated that they then rely on the risk register for the residual risk assessment (four respondents). The assessment of the residual risk is dependent on the current mitigation activities in place (refer to sections 3.4.4.1 on p. 190 and 3.4.4.2 on p. 190) and it therefore does not make sense to use the risk register for the residual risk assessment but not for the current risk mitigation activities.

- **Underdeveloped areas**

According to the literature (refer to section 4.5.4.2 on p. 270), when comparing the second COSO model with the fourth generation internal audit engagement process (refer to table 4.5 column 6 on p. 272), five specific underdeveloped areas are identified. Some of these limitations are addressed above. However, three of these underdeveloped areas remain, namely that:

  - both threats and loss of opportunities are identified as possible risks;
  - a risk(s) may have an effect on another area (outside the scope of the engagement), equally a risk(s) in another area (outside the scope of the engagement) may have an effect on this engagement;
  - activities other than controls to mitigate risk to an acceptable level are considered.

These were investigated by obtaining the views of the respondents and the results are summarised in table 5.32 on p. 355.

Table 5.32: Underdeveloped areas in a risk-based internal audit engagement

Both threats and loss of opportunities are identified	Effect of risk in engagement on another area	Effect of another risk on engagement	Recommend other risk mitigating activities (not controls)
4	5	5	2

The results reflecting on the first underdeveloped area, namely the identification of both threats and loss of opportunities as risks, are in line with the results in table 5.27 on p. 349. However, the results reflecting on the second underdeveloped area (refer to the second and third column of the above table) contradict the results in table 5.23 on p. 344, which indicates that only two organisations have an integrated organisation-wide risk management process, as well as table 5.31 on p. 353, which indicates that internal auditing relies on the risk register of the risk department (only two respondents should have an organisation-wide risk register in place). The last weakness, namely that internal auditors are cautious to recommend other risk mitigating activities than controls, are relevant to this study.

Further comments made by the respondents on the risk-based planning of internal audit engagements include the use of CAATTs to assist in the identification and assessment of risks, using information that is obtained by combining the information in the risk register and the internal auditor's own risk assessment, that the risk department's systems are not mature enough to perform a comprehensive risk-based internal audit engagement as per COSO II methodology, and the fact that risks are still treated within a silo instead of part of organisation-wide integration.

5.3.4.4 Risk-based internal audit model

In section 5.3.1.4 on p. 312 the rationale behind the preliminary risk-based internal audit model that has been developed and the inclusion of input from the respondents to refine the model is discussed. In this section the results of the

respondents' input into the model that were obtained are summarised, analysed and discussed.

- **Benefits of the model**

In theory, it seems that the preliminary model (refer to section 4.5.5 on p.274) has many benefits. However, the proof is whether internal auditors will be able to apply the model in a practical situation and whether the benefits exceed the cost and/or effort to implement the model for a specific internal audit function. Table 5.33 below gives the views of the respondents.

Table 5.33: Viewpoints of the use and benefits of a risk-based internal audit engagement model

Benefits	Number of respondents
Model can be used during internal audit engagements	5
Model will reduce the extent of engagement procedures performed	5
Model will be effective in focusing on the crucial aspects	5
Model will be efficient (e.g., save time) whilst still being effective	5
Model will assist in eliminating ineffective controls	5
Model will assist in eliminating unnecessary controls	5
Model will assist in eliminating redundant controls	5
Model will assist in eliminating excessive controls	5
Model will assist in simplifying complex controls	5

All the respondents agree that the model would certainly benefit the internal audit function overall, but more specifically the quality of an internal audit assurance engagement. Apart from the above indications, further comments related to the use of the model include:

- respondents are concerned that risk management systems are not mature enough to accommodate the model;
- it is difficult for internal auditors to eliminate over-controlling (refer to a discussion on this topic in section 4.3.3.2 on p. 249);
- internal auditors tend to over-audit to protect themselves;
- valuable internal audit resources should not be wasted on areas that are not effectively controlled by management; and

- audit engagements can and should be more focused.

- **Low inherent risks**

The preliminary risk-based internal audit engagement model bases the exclusion of an activity with a low inherent risk from the engagement on the assumption that the risk is not material to the organisation (refer to risk number 9 in figure 4.4 on p. 279). The study's respondents were asked to comment on this assumption and their views are summarised in table 5.34 below.

Table 5.34: Treatment when the inherent risk is low

Inclusion in engagement planning	Number of respondents
Full inclusion	0
Only partial inclusion (based on judgment)	1
Only on surprise basis	1
No inclusion	3

The majority of the respondents (three respondents) were of the opinion that these risks should not be included in the audit engagement scope as this is a waste of scarce internal audit resources. Even where inclusion was suggested, this was only either based on the internal auditor's judgement, or on a surprise basis, for example, when fraud is suspected.

- **Inherent and residual risk above risk appetite**

In the preliminary risk-based internal audit engagement model the assumption is made that when both the inherent risk and the residual risk are above the risk appetite the activity should not be audited, instead the lack of sufficient risk-mitigating activities should be reported to management. Only controls that do mitigate the risk effectively and efficiently should be investigated (refer to risk number 2, 3, 4, 6 and 8 in figure 4.4 on p. 279). The views of the respondents are summarised in table 5.35 on p. 358.

Table 5.35: Treatment when the movement of inherent to residual risk is unsatisfactory

Inclusion in engagement planning	Number of respondents
Must be included in full (audit all controls)	0
Only focus on adequacy of relevant controls	3
Only focus on effectiveness of relevant controls	4
Only an audit finding	1

Most of the respondents agreed (four of the five) that the operational effectiveness of relevant controls that do mitigate the risk should be included; the respondents also (three of the five) felt that the investigation as to the adequacy or design effectiveness of such controls should also be performed. However, the fact that the residual risk is above the risk appetite should at minimum require a discussion with management on why the controls are not lowering the risk to an acceptable level, or even constitute an audit finding.

Further comments on the model included:

- Internal auditing must first audit the risk department and the risk management process before it can rely on the outcome, as documented in the risk register.
- Internal auditing should track risks that are not included in the audit scope to ensure that it is still correctly assessed (for example, low inherent risks).
- Management should sign off a document that stipulates that they are aware of, and accept the high residual risks, and this document should then be attached to the audit report.
- Internal auditing could keep track of management's action plans as well as the impact on the organisation for high residual risks.

5.3.5 Conclusion

In this section, the results of the second empirical study are discussed. The views of the top five highest risk mature score organisations' chief audit executives of both the private and the public sectors were obtained on various aspects. A brief

discussion on the results of each area is provided. Further interpretations of the results, especially on how the results could be used to improve the risk-based internal audit engagement model (private sector), or the improvement of the risk maturity of organisations (public sector), are debated in Chapter 6.

In the next section, the preliminary model is tested in a practical situation. The model is then adapted to incorporate the findings of the chief audit executives obtained during the interviews, as well as the problems encountered during the practical application and the perceived limitations and benefits of the model.

5.4 TEST THE MODEL (CASE STUDY)

Chapter 4 details the development of a preliminary model, based on the literature, to perform risk-based internal audit assurance engagements. In section 5.3 the input obtained from participating chief audit executives regarding the usability of the model at private sector risk mature organisations is given. Included in the information obtained are the views of the respondents on how the model can be refined. In this section the third empirical study, namely the testing of the model at a specific organisation using the case study methodology, is described. Apart from the results of the empirical study the section outlines the motivation for choosing a specific organisation, the criteria that were needed to be able to perform the testing, the identification of a specific audit engagement as the test sample, the structure of how the case study was conducted, the scope of the case study, and certain limitations experienced before and during the execution of the case study. Where applicable, the relevant literature discussions as per Chapters 2, 3 and 4, as well as the research methodology followed as per Chapter 1 are referred to.

5.4.1 Criteria for test sample(s)

Section 1.8.4.2.3 on p. 51 – Population and sample, states that one organisation in each sector will be included in the testing of the model. These organisations would be chosen using the following criteria, guided by professional judgement:

- the risk maturity of the organisations in each sector;
- the organisation in each sector with the highest risk maturity score;
- the input received from the respondents of the ten organisations interviewed, for example, refer to the required criteria when testing the model (section 4.5.3 on p. 264); and
- the willingness of the organisation to participate in the case study.

In section 5.2 on p. 301, the risk maturity scores of the organisations in the private and the public sectors (refer to section 1.8.4.2.1 on p. 44) are documented. For the public sector, all the organisations that were included in the sample were risk immature, thus excluding this sector from the third empirical study. The five private sector organisations with the highest risk maturity score were included in the second empirical study. However, only one organisation met all the requirements needed to perform the case study as mentioned above. Due to the confidentiality agreement with the organisation, it will be referred to in this study as Company X.

5.4.2 Additional required criteria and information

In section 4.5.3 on p. 264, the three basic elements that are needed to perform a risk-based internal audit engagement are identified and discussed. In section 4.5.5 on p. 274, the assumptions that were made when developing the preliminary model are discussed. The following is a summary of these points:

- The organisation should be risk mature.
- The risk management process should be performed for operational activities.
- The organisation should have a comprehensive and up-to-date risk register that includes the outcome of both strategic and operational risk management processes.
- The risk appetite and risk tolerance levels have been set by management and/or the board.

- The risk management process has been audited by the internal audit function and the outcome of the process(es) performed can be relied upon by internal auditing.

All these criteria were relevant to the five private sector organisations included in the second empirical study. However, to be able to test the model's effect on an internal audit engagement's effectiveness and efficiency, an audit engagement previously performed by the organisation without having the input of the operational risk management process as documented in the risk register was needed as test sample. This audit engagement had to still be relevant and had to have been performed recently, preferably in the current or the previous financial year. As indicated in the previous section, Company X met the basic criteria for the test sample (refer to section 5.4.1 on p. 359). It also met all the above additional criteria.

5.4.3 Criteria for choosing an audit engagement

Apart from the requirements used to determine which organisation to include in the case study, as discussed in the previous two sections, further detailed criteria were used to determine which audit engagement would be suitable as the test sample (refer to section 1.8.4.2.3 on p. 51 – Population and sample):

- The organisational operational area included in the audit engagement must be a high strategic risk for the organisation.
- The audit engagement performed must be an assurance engagement, thus excluding consulting services performed by the internal audit function.

A further point to consider is that Company X has certain specialised and highly technical operational areas. The auditor that was to carry out the case study is not employed by this organisation and it would have taken time for that person to gain a comprehensive understanding of such a technical area. Therefore, the operational area covered in the internal audit engagement that was to be

included in the case study had to be understandable to a general internal auditor and not be focused on these highly specialised or technical areas.

Further detailed information that was required included the system description, the audit plan as documented in the engagement programme with its detailed engagement procedures, and the final audit engagement report with its detailed audit findings. Lastly, the current risk register with all the detail as stipulated in section 3.5.3 on p. 203 for the specific operational area was required.

5.4.4 Structure of the case study

After all of the above criteria were met and the relevant information and documentation were obtained, the execution of the case study was planned as follows:

- A clear understanding of the system description was obtained.
- The audit procedures performed during the engagement were listed.
- The individual audit findings were examined and summarised.
- The current risk register for the operational area was obtained.
- The risks as per the risk register were classified as follows (refer to the research objectives in section 1.8.2 on p. 40):
    - high/moderate inherent risk areas that had lower risk levels after controls were implemented (residual risk);
    - low inherent risk areas; and
    - high/moderate inherent risk areas that remained at high risk levels after controls were implemented (residual risk).
- The following criteria were used to determine how the inherent risks and the controls as per the risk register should be included in the audit engagement's list of engagement procedures:
    - The controls for high/moderate inherent risk areas that had lower risk levels after controls were implemented should be included in the audit engagement programme.

- The controls for low inherent risk areas should not be included in the audit engagement programme.
- The controls for high/moderate inherent risk areas that remained high risk should not be included in the audit programme but be reported to management (audit finding in the audit report).

- The above list of engagement procedures were compared to the original list of engagement procedures to determine whether fewer tests would have been performed if the risk-based model was used.
- The list of engagement procedures was compared to the original engagement findings as listed in the audit report to determine whether all the relevant audit findings would have been discovered had fewer tests been performed.

Although all possible precautions were taken while planning the case study as well as the field work, many problems were encountered during the execution. These, as well as the results of the execution of the study, are documented in section 5.4.6 on p. 364.

5.4.5 Case study's scope and limitation

The overall scope and limitation of the entire study is discussed in section 1.8.3 on p. 41. For this empirical part of the study – the case study – a few additional points regarding the scope and limitations are discussed. Firstly, only the private sector was included in the testing of the model due to the fact that none of the public sector organisations was risk mature (refer to section 5.2 on p. 301) and this is one of the requirements to implement the model (refer to section 4.5.3.1 on p. 264). In the second place, it is difficult for a general internal auditor to obtain a comprehensive understanding of a specific organisation's systems and processes within a short period of time. Although this was adjusted for by choosing an audit engagement performed on a generic rather than technically specific area, it could still be possible that the level of understanding of the systems and processes was not wholly sufficient. Thirdly, there was a time restriction due to the fact that the working papers are kept electronically and no copy of the file or hardcopies were

allowed to be removed from the premises. The case study had to be performed at the organisation's premises and at a time that was convenient for them. The audit engagement that was chosen had to be large enough for a meaningful test to be performed, but at the same time not too large due to the time constraint.

5.4.6 Result of the case study

The result of the case study performed is provided in this section. However, a few problems were encountered during the execution of the test and these will first be discussed.

5.4.6.1 Problems encountered during execution

Apart from the general limitations experienced in the planning and the execution of the case study as discussed in section 5.4.5 on p. 363, a few difficulties were encountered while performing the steps of the case study plan as mentioned in section 5.4.4 on p. 362. These are summarised in table 5.36on p. 365 in the context of how the problem was managed by the researcher while performing the test, as well as the effect of the problem on the outcome of the case study.

Although the problems had an effect on how the model was implemented during the case study, it was possible to manage them without compromising the quality of the test.

Table 5.36: Problem encountered during the testing of the model

Problem	Managed by researcher	Effect on case study
Audit working papers had limited information on the detailed audit procedures performed on a specific process – the information mainly consists of walk-through tests with visual print-outs of the electronic system to explain the flow of the system	Where applicable, the description of the process and the controls that should be in place according to the working papers were used instead of the audit procedures	It was not possible to list all the steps in the process (including the controls) as audit procedures. The main steps within the process were used as the basis
For the specific process, both strategic and operational risks were combined in one risk register	The classification was ignored and professional judgement was used as to whether to include the risk as operational or strategic	Some of the strategic risks have an influence on the operational process and were therefore included in the test
The risks listed in the risk register did not cross reference to the operational process	Each risk documented in the risk register had to be classified in accordance with the steps in the operational process	Many of the process steps were not addressed in the risk register. This was a concern for the implementation of the model
The risk assessment methodology in use was very limited (only low, medium and high) with no indication of risk tolerance/appetite	All movement between risk levels was used including high to medium as well as medium to low as possible effects on the audit procedures	If the risk assessment had been more refined it would have had a further positive effect on the elimination of unnecessary audit procedures and the identification of over-controlling

5.4.6.2 Discussion of results

In table 5.37 on p. 367 the results of the case study structure as described in section 5.4.4 on p. 362 are summarised. In the first column the process areas are numbered as per the audit programme. In the second column the number of risks, as listed in the risk register, applicable to each process area is listed. The word 'General' in column 1 refers to a risk that is applicable to all the areas. In column three the difference between the inherent risk and the residual risk

indicates whether the movement warrants an inclusion in the audit programme as per the model (refer to section 5.4.4 on p. 362 for the criteria used to determine whether audit procedures should be included in the audit engagement or not). In the next section, 'Influence on audit procedures performed', the table differentiates between procedures currently included (walk-through tests were mainly used and these are excluded from the analysis), procedures included if the risk-based audit model is used and the nett effect on the audit programme. In the section on audit findings, the results as to whether findings would have been identified when only performing the audit procedures as per the risk-based audit model are investigated as well as the possible inclusion of further audit findings and/or discussions with management.

The overall results of the case study indicate that if the model was used, less audit procedures would have been performed but that all the audit findings would still have been included in the audit report. The process area 'General' mainly refers to strategic-type risks that reflect on all the other process areas and were not included in the initial audit scope. However, if these were to be included, the value that internal auditing could add rises even further. Furthermore, a few additional audit findings could most probably have been identified which, for this specific case study, include areas where weak controls exist, over-controlling, and other more strategic weaknesses or problems that need to be brought to management's attention.

5.4.7 Conclusion

In this section the results of the third empirical study are summarised and briefly discussed. Although many problems and shortcomings were identified during the execution of the case study the results support the use of the preliminary risk-based internal audit model when performing an assurance internal audit engagement.

Table 5.37: Summary of results of the case study

Process area	Number of risks as per risk register	Movement indicates inclusion (refer to section 5.4.4 for reasons)	Influence on audit procedures performed			Audit findings		Additional finding or discussion		
			Currently included	After use of model	Nett effect	Currently included	Use of model	Over control	Weak controls	Other (**)
1	4	2	4	2	Less	None	N/A		2	
2	6	3	5	3	Less	Finding 1	Yes		2	
3	4	2	4	2	Less	None	N/A		2	
4	5	1	4	1	Less	None	N/A		4	
5	6	3	3	3	Same	None	N/A		1	1
6	2	2	2	2	Same	None	N/A			
7	4	2	4	2	Less	Finding 2 Finding 3(*) Finding 4	Yes Yes Yes	1	2	
General	10	4	0	4	More	Finding 5 Finding 5	Yes Yes	1	1	4

(*) – Finding 3 not accepted by management as it is too difficult to implement a solution

(**) – 'Other findings' refers to risks that are high and should be brought to management's attention in order that they may be addressed accordingly

In the next section, the results of the second empirical study (refer to the previous section) as well as the third empirical study, as discussed in this section, are used to refine the preliminary model that was developed based on the literature (refer to section 4.5.5 on p. 274).

5.5 REFINE THE MODEL

The lay-out of the risk-based internal audit engagement model is revisited by using the preliminary model (refer to section 4.5.5 on p. 274) with specific reference to table 4.6 on p. 275) as a basis and then incorporating the input received from chief audit executives during the second empirical study (refer to sections 5.3.4.3 on p. 351 and 5.3.4.4 on p. 355), as well as the results of the case study as discussed above. This comparison and the effect on the model are summarised in table 5.38 on p 369.

A few important aspects that should be mentioned with regard to the refinement of the model are as follows:

- Although the respondents were under the impression that they were following a COSO II methodology, the fear of not covering all the required aspects of the engagement, and being 'caught-out' by management should they not identify all the relevant weaknesses, as well as other problems, were the motivation for still following the more comprehensive COSO I audit methodology.
- It is of the utmost importance to first audit the risk management process methodology before internal auditing can rely on the outcome of the process, whether for the incorporation of strategic risks as part of the internal audit function's annual plan, or for the use of operational risks as part of the internal audit engagement.
- For both strategic and operational level risk, both the threats as well as the loss of opportunities should be included in the risk management process. Even if management has excluded the latter the internal auditor should include these as part of the internal audit engagement.

Table 5.38: Comparing the preliminary model, input received from CAEs and the results of the case study

Step	Internal audit engagement planning based on literature (refer to table 4.6)	Input from CAEs	Result of case study	Influence on model
1	• The activity's objectives and related criteria form the foundation of the audit engagement objectives and scope: o Review the objective setting process and outcome and, if needed, identify further objectives, or only focus on priority objectives (based on the audit resources available) o Set the engagement objectives and scope	• Use auditee input • Use the risk management processes' results • If no or limited information exists, the internal auditor should obtain further information • Methodology followed is mainly COSO I methodology although repsondents initially thought it was COSO II based	• Not applicable	• Ensure that COSO II methodology is followed
2	• The risks threatening the activity's objectives form the foundation of the engagement planning: o Consider the risk identification process and all relevant exposures identified according to the process o While obtaining knowledge of the activity, consider other exposures and risks for both hazards and opportunities threatening the reaching of the activity's objectives	• Use the previous year's working papers as a starting point • Internal auditing should perform an audit to verify the effectiveness and results of the risk management process, including operational risks • Both threat and loss of opportunity are considered	• For operational level: o Only threats are considered • For strategic level: o Both threats and loss of opportunities are considered	• Audit the effectiveness and outcome of the operational risk management process • Both threats and loss of opportunities must be considered as risks during the planning phase of the audit engagement

Step	Internal audit engagement planning based on literature (refer to table 4.6)	Input from CAEs	Result of case study	Influence on model
3	• Both the inherent and residual risks are assessed (likelihood and impact): o Consider the risk assessment process and use outcome or perform own assessment o Review inherent risk level, current risk responses in place, and residual risk level for each risk o Measure inherent and residual risk levels in the context of the risk appetite o Focus more on high level risks (inherent risk exceeds the risk appetite) o For the engagement programme, include current existing responses where the inherent risk is high but the residual risk is within the risk appetite levels o Investigate whether these responses are functioning as planned o Consider low inherent risk for inclusion in the engagement programme by using professional judgement o Consider high inherent risk where the	• Use risk management process results for: o inherent risks; o difference between inherent and residual; and o measurement or assessment of inherent and residual risks • Perform own risk assessment (additional) • Consider enterprise risk management integration: o Effect of risk on another area o Effect of another risk on this engagement • Internal auditor does not rely on the current risk mitigation activities as per the risk register, and, as such, focuses only on controls • No inclusion of low inherent risks • When the residual risk is still too high, evaluate control	• Use risk management process results as a basis for engagement planning • Focus on the high/ moderate inherent risk levels • Focus on areas where the movement between inherent and residual risk is material • Focus on the areas where the residual risk is within the risk appetite (moderate to low) • Focus only on the risk mitigation activities of the risk management process • No inclusion of low inherent risks • Residual risk that remains high is not included in the audit engagement o Less audit procedures	• Use preliminary model as discussed in section 4.5.5 • Perform own risk assessment only if no risk management process exists or if it is not reliable • Consider integration of risks with other areas • Include other areas of risk mitigation, e.g., outsourcing • Ignore low inherent risk areas • Investigate control effectiveness, and if applicable, adequacy for high residual risks

Step	Internal audit engagement planning based on literature (refer to table 4.6)	Input from CAEs	Result of case study	Influence on model
	residual risk remains high for inclusion in the engagement programme by using professional judgement	effectiveness and, if applicable the adequacy	are performed ○ All findings as per the audit report are identified ○ Additional findings and/or areas that need to be discussed with management are identified	
4	• The assessment of each risk is measured in terms of the risk appetite • Residual risk exceeding the risk appetite must be further treated by means of an appropriate risk response: ○ Consider engagement recommendation in terms of the appropriate risk response ○ Include in the follow-up phase of the engagement	• Perform an investigation of the control effectiveness for residual risks above the risk appetite • Consider management signing a document where they acknowledge that they are aware of the high residual risk • Internal auditing keep track of management's action plans and the impact on the organisation	• Residual risk that remains high is not included in the audit engagement: ○ All relevant findings are identified ○ Additional findings that should be brought to management's attention are identified	• Additional findings and/or areas that need to be discussed with management are identified

CAE – Chief audit executive

- Internal auditors still tend to perform their own risk assessment instead of relying on the risk management process. If internal auditing has provided assurance on the risk management process, however, then there is no reason not to trust the risk management process's outcome for the identification, assessment and mitigating activities as documented in the risk register. If the engagement reveals otherwise, this information should be used to update the risk register.
- Some organisations have not fully developed their integrated risk management processes, this then makes it difficult for the internal auditor to incorporate risk outside the audit scope into the engagement, or risks identified during the engagement that have an effect on another area into that audit engagement. This widened risk-incorporation process can only be fully implemented by the internal audit function when the risk department is focused on the integration of organisation-wide risk management. Until such time, the internal auditor should be aware of the weakness in the methodology and, where applicable, refer to risks outside the scope of the audit or incorporate risks identified in this engagement into a later engagement.
- Internal auditors are known as control experts and are used to providing recommendations on controls. However, sometimes it is more effective and efficient to suggest another form of risk mitigation such as sharing the risk or eliminating the activity that gives rise to a specific risk.
- The empirical studies' results indicate that low risks should not be included in the internal audit engagement, not even on a surprise basis. Thus, if the risk management process can be relied upon, low inherent risks should be eliminated from the engagement scope. However, it is suggested that the internal auditor should always use professional judgement when making this decision as some low risk areas could lead to other risks arising, such as fraudulent activities.
- High inherent risks should only be included by investigating the control effectiveness, that is, the extent to which the control minimises the risk. Only those controls that do add to the risk mitigation should be investigated

for the adequacy of the control – the extent to which the control is implemented and properly carried out.

- If the risk-based internal audit model is used correctly for the performance of an internal audit engagement, more audit findings could most probably be revealed (refer to table 5.37 on p. 367). These could include formal findings that should be reported in the audit report, or, otherwise, aspects that must be brought to management's attention for them to decide whether each should be addressed or not, constituting an informal finding or discussion that is addressed on an interim basis and is not included in the final audit report.

5.6 CONCLUSION

In this chapter the results of the three empirical studies have been presented and discussed. In the first study the risk maturity of each of the target organisations was measured against a risk maturity scorecard, based on a pre-developed risk maturity model that was adapted for SA organisations. It is evident from the results of the study that the participating public sector organisations lack risk maturity.

In the second empirical study the results of the interviews with the chief audit executives of the top five risk mature private sector participating organisations were used to get insight into the organisations' risk structures and internal audit functions' risk activities, and input into the risk-based engagement model. From the results of the study it is evident that although internal auditing is playing its role in the risk management of the organisation a few areas could be further developed, including the use of a structured risk-based model when performing internal audit engagements. For the public sector, five chief audit executives of the seven highest risk mature participating organisations were interviewed, mainly to get insight into why these organisations were not risk mature. The results indicate that the risk management structures within these organisations are fairly new and thus still in a developing phase. Also, the lack of resources within the internal audit functions is a major concern for these chief audit

executives, and is hindering the functions in executing their duties with regard to the management of risk as stipulated in the relevant guidance.

In the third empirical study the risk-based internal audit engagement model was tested using a case study. The planning phase of an internal audit engagement that was performed previously was re-performed using the model's methodology. The results indicate that if the model had been used in executing the engagement fewer audit procedures would have been performed, but at the same time more audit findings would have been uncovered – thus proving that the risk-based internal audit model for assurance engagements will ensure that audits are performed more effectively and efficiently.

In the next chapter, the results of the three empirical studies will be discussed in the context of the research problem and objectives as well as the literature review. A final conclusion will be provided as well as recommendations on the weaknesses and limitations of the current methodology followed when performing an internal audit engagement. Lastly, potential further research areas will be listed.

CHAPTER 6
CONCLUSIONS AND RECOMMENDATIONS

6.1 INTRODUCTION

In Chapter 5, the detailed results of the three empirical studies are presented, resulting in the chapter being a lengthy document. It was decided to provide the discussion on the elaboration of the results in a separate chapter. In this chapter, the main findings of the literature review as well as the results of the three empirical studies are summarised and, where appropriate, integrated. Recommendations for improvement are made, possible further research areas that have been identified during the execution of this study are listed, and conclusions are reached in line with the research problem and research objectives as stipulated in Chapter 1. A final conclusion of the study is provided.

6.2 NEED FOR CHANGE IN THE WAY INTERNAL AUDIT ENGAGEMENTS ARE PERFORMED

In Chapter 1 the need for this study is debated. There are many reasons, both past and ongoing, why internal auditors need to perform internal audit engagements more effectively and efficiently. The first contributing factor to this study is the changing internal audit environment, especially the growth within the internal audit profession, which, whilst it is expanding, is not adequately fulfilling the need for competent internal auditors. The second factor that necessitated this study is the influence of the constant development of corporate governance guidance and legislation, both globally and in SA, especially in the areas of internal auditing and risk management. Thirdly, the external audit and internal audit professions should work more closely together to improve coordination, eliminate duplication and provide combined assurance to the organisation. They should be able to rely on each other's work. A structured and systematic approach in performing internal audit engagements could result in the external auditors placing more reliance on the work of the internal auditors. Lastly, the

question as to whether the study should focus on both the private as well as the public sector is debated. It is concluded that internal auditing is a principle-driven profession, and although the environment in which the two sectors operate may differ, the similarities of the internal audit profession within the two sectors necessitated that both be included in the scope of the study.

With the changing environment in which internal auditors operate as indicated above, as well as the overall complexity of the business environment and the constant emerging of new risks threatening the achievement of operational objectives, internal auditors need to adapt the way they operate. One of these changes is the implementation of risk strategies into internal audit engagement methodologies. It is concluded in Chapter 1 that the governing body of the profession, namely the IIA, has provided limited guidance to their members on this topic, hence the need for further guidance.

The literature study first investigated the debate on the evolution of the internal audit profession (refer to Chapter 2). Sections 1 and 2 (refer to Annexure I on p. 481 and J on p. 491) of the second empirical study (refer to Chapter 5 for the results) addressed certain of the issues identified. These results will be discussed in the next section.

6.3 THE EVOLUTION OF INTERNAL AUDITING

In Chapter 2 of the study the evolution of the profession is first debated in the context of the history of the profession as well as the theory of internal auditing. It is concluded that the IIA, with the IIA Inc. as its head office and its network of chapters across the globe, is positioned in such a manner that it is globally competitive yet locally relevant. Furthermore, the profession plays a crucial role in the accountability and agency theories within organisational structure. The structuring and functioning of the internal audit function are influenced by the guidance provided by the IIA (especially the revised definition), internal organisational factors and external factors.

Specific areas that greatly affect the internal audit function include the following:

- The increase in consulting activities performed by the internal audit function could decrease the resources available to perform assurance activities. Cost restrictions or a lack of knowledge and skills amongst the internal auditors could lead to outsourcing the function, or to co-sourcing (that is an in-house function partly outsourcing certain activities).
    - The empirical study's results indicate that both the private and the public sectors perform more assurance than consulting engagements – this is in line with the spirit of the profession.
    - The public sector internal audit function has a higher tendency to outsource activities.
        - This could be related to the fact that most of the private sector organisations that participated in the study are bound by regulations, according to their specific industry, that do not allow such outsourcing.
        - Reasons for the tendency to outsource include that the public sector organisations have smaller internal audit budgets and thus a smaller staff complement, resulting in a limited pool of skills and knowledge.
- The internal audit universe is expanding due to the incorporation of governance and risk management principles. The IIA has developed additional guidance on these areas, especially risk-related topics.
    - The empirical study's results underline the fact that private sector organisations do adhere to the IIA *Standards* – specifically those that address risk management, the planning of the function's activities based on a risk assessment, and risk-based internal audit engagements. With regard to performing consulting engagements to improve risk management, the respondents were of the view that their organisations' risk management frameworks were well developed and did not need further assistance.

- Public sector organisations are not fully adhering to the IIA *Standards*, especially with regard to the organisation's risk management framework.

- There is a lack of competent and skilled internal auditors, especially in the specialisation fields of IT and risk management.
  - Both the private and the public sectors' internal audit staff complements are higher than the norm for global private sector internal audit functions.
  - With regard to tertiary qualifications, professional qualifications and internal audit experience:
    - the private sector organisations' staff are well qualified but have limited internal audit experience; and
    - the public sector organisations' staff are under-qualified, especially with regard to professional qualifications, but have ample internal audit experience.
  - When internal audit duties in respect of the risk management framework, including the risk management process, are performed, contradictory to what the literature concludes, consultants or experts are not contracted to perform the task.
- The status that the internal audit function enjoys within the organisation can be linked to the reporting lines of the chief audit executive, the position of the function within the organisation, and the budget in relation to the organisational financial indicators and external audit fees.
  - To enhance independence, SA guidance indicates that the chief audit executive should report functionally to the audit committee. SA legislation for the public sector elaborates on this guidance by stipulating that the chief audit executive should also report administratively to the Director General.
    - With regard to the private sector organisations, their administrative reporting structures could pose a threat to their functions' independence with most chief audit executives reporting to their chief financial officers.

- The public sector organisations' reporting structures are in line with legislation.

- Although most organisations' internal audit functions are positioned as a separate function within the organisational structure, there is a concern that the independence of some of the respondents' internal audit functions could be jeopardised as a result of these functions being situated in especially the financial section of the organisation.
- Both the private and the public sectors' budgets in terms of revenue (private sector) and expenditure (public sector) are higher than the norm for global private sector internal audit functions.

How an internal audit function reacts to the above changes and influences will have a direct effect on how other stakeholders perceive, and ultimately utilise, the function. Whether management establishes an internal audit function merely as a corporate governance requirement, or management over-utilises the function, the role of internal auditing is changing. Further factors influencing this role are the current financial crisis affecting the profession in a positive (management asking for an increased focus on risk management) as well as a negative (less internal audit resources) way, and the growth in the use of technology (CAATTs), both by the organisations (internal audit needs to provide assurance) and by internal auditors.

In the next section the development of corporate governance, with specific reference to risk management, is discussed in the context of the literature study (Chapter 3), the first empirical study (refer to Annexure B to H on pp. 459 to 479 and Chapter 5 for the results), and the second empirical study (refer to section 1 in Annexure I on p. 481 and J on p. 491 and Chapter 5 for the results).

6.4 RISK MANAGEMENT AS PART OF CORPORATE GOVERNANCE

Corporate governance is not a new concept – it has been much debated over the last two to three decades (refer to Chapter 3). Two of the cornerstones of sound governance principles are internal auditing and risk management. Risk management is a tool that management and the board can use to ensure that the

organisation's objectives are met. The literature study concludes that the implementation of an effective risk management strategy has a positive effect on investors' decisions. Internal auditing should provide assurance to these parties that the organisation's risk management is effective in the achievement of its goals and is efficiently implemented within the organisation. Although a relatively new concept to the greater business environment, risk management has grown tremendously over the last few years with much new guidance and legislation addressing the topic. Two specific areas that need further development include the use of common terminology for the various concepts, as well as integrated risk management (holistic approach) instead of treating risk within silos.

Organisations need to benchmark their risk management strategies against best practices to ensure that their strategies are addressing all their needs, as well as to check the effective implementation of the identified and necessary risk management elements. One way of doing this is to measure the organisation's risk maturity. The empirical study's results indicate the following trends:

- The overall risk maturity of the participating organisations, measured against a pre-developed risk maturity model that was adapted for SA organisations, indicated that:
    - private sector organisations are on average risk mature with thirty of the forty organisations in the sample being risk mature; and
    - not one of the thirty-six private sector organisations was risk mature, a concerning fact for this sector as legislation enforces risk management for these organisations.
- The two attributes that received the lowest score for both the private and the public sectors' organisations are the organisational culture not supporting the management of risk, and staff not being equipped and supported to manage risk well. This is in line with the literature study that indicates that there is a lack of management commitment to risk management.
- For both the sectors, the internal audit function's role with regard to risk management was evaluated above the overall risk maturity score for all the

organisations within the sample, and even more so for the top five private sector and top five public sector organisations within each sector.

- When discussing the risk maturity score with the participating organisations during the execution of the second empirical study:
    - the private sector organisations agreed with the risk maturity score as calculated in the first empirical study; however
    - only one public sector organisation agreed with the risk maturity score, confirming the fact that risk management is not well developed in the public sector, or that various role players (such as internal auditing) are unsure of the true status of risk management within their organisations.

Various parties should take responsibility for the establishment and functioning of an effective and efficient risk management framework (that is the totality of all structures, processes, systems, methodologies and individuals involved in implementing a risk management strategy). The board or executive management, which is responsible overall for the implementation of risk management and accountable to stakeholders, delegates this duty to a board risk committee as well as other internal risk structures. The empirical results lead to the following conclusions:

- Audit committees are well established in all the participating organisations. However, the fact that some organisations indicated that their organisational structure comprises a combined audit and risk committee could indicate an area for improvement, as the existence of separate committees could further enhance the management of risks.
    - The composition of the public sector organisations' audit committees in terms of their members is not fully in accordance with the King Report's guidance.
- The organisations' risk management structures are in a development phase and many organisations are still deciding which options to follow.
    - The private sector organisations participating in the study have most of the risk structures in place.

    - The public sector organisations do not have comprehensive risk structures in place. The respondents indicated that risk management processes (that is the steps followed to identify, assess, treat, monitor and report on risks) are implemented on strategic and operational levels (and even organisational-wide for two respondents) by their chief risk officers – it is difficult to believe that these processes are performed effectively by one individual in each company.
- With regard to the reporting lines of the risk management structures, senior management and the board are still unsure as to where these functions should be positioned within the organisational structure.

As mentioned above, many parties within the organisational structure are responsible for the management of risk, of which the risk committee, the audit committee, internal risk structures, as well as internal auditing all play important roles. Proper communication and coordination between these parties will ensure that risk will be managed to the best of the organisations' abilities. The respondents indicated the following:

- Proper communication lines exist between internal auditing and risk management structures within both the private and the public sectors' organisations. The public sector organisations further indicated that internal auditing and risk management structures assist one another with their respective duties. However, the question remains as to how effective the communication channels are, especially in the light of continuous scandals in both these sectors.
- It is concerning to note that only two private sector organisations and no public sector organisations have separate board audit and risk committees and that the only interaction between them is that at least one member of each committee serves on the other committee as well.
- Coordination between the risk, or the audit and risk committee, and internal auditing does exist.
    - This interaction is well established in the private sector.

- For public sector organisations very limited coordination exists and this is an area that needs urgent attention.

The risk management framework consists of various elements – one being the risk management process performed on various levels of the organisation, the results of which are documented in a risk register. The respondents' information highlights the following trends:

- With regard to the risk management process, the respondents' organisations do have such processes in place for strategic and operational levels, with the outcome of the process being electronically documented in a risk register. However, organisation-wide integration processes are still lacking.
- The risk department is the main party responsible for the implementation and execution of the risk management process on all levels of the organisation. Where an organisation has a risk department and a chief risk officer, the department takes the responsibility for the implementation of the risk management processes at various organisational levels.
  - However, as mentioned before, it is concerning to note that most public sector organisations only have a chief risk officer that has to implement the process on both the strategic and operational levels. The question is whether one person could perform this task properly.
- Risk registers are on average updated on a monthly basis. Although this seems adequate, more improvement is possible. The organisations that do have a risk register in place indicated that they use specialised software programmes that allow updating on a continuous basis.

From the literature as well as the results of the empirical studies, it is evident that risk management, although currently in an evolving phase, needs to be implemented properly in organisations. The public sector organisations in particular indicated that much has to be done to get the proper structures in place. In the next section, how internal auditing is incorporating risk-related concepts into their duties is summarised, referring to the literature (Chapter 4) as

well as the second (refer to section 3 to 8 in Annexure I on p. 481 and J on p. 491 and Chapter 5 for the results) and the third (refer to Chapter 5 for the results) empirical studies.

6.5 THE ROLE OF INTERNAL AUDITING WITH REGARD TO RISK

As mentioned above, internal auditing, according to the literature as well as corporate governance guidance, is one of the parties with a role to play in corporate governance in general, and more specifically the management of risks of the organisation. In Chapter 4 of the study the literature on this topic is discussed, and three main areas are identified. However, before these can be discussed here, the views of the chief audit executives interviewed in order to understand how the changing internal audit environment has affected the responsibilities of the function towards the management of risk in general are restated. The results are summarised below:

- The chief audit executives are of the view that internal auditing should perform assurance services with regard to the risk management framework (including the risk management process), but should not take responsibility for it.
- With regard to the current as well as future involvement of the function, the chief audit executives interviewed had the following viewpoints:
    - The private sector chief audit executives regard the second King Report as the key instigator for the increased involvement of internal auditing in the management of risk. King III as well as the board's changed needs will most probably be important to guide future involvement. The current financial crisis was not mentioned, probably as a result of the view, right or not, that it has not affected the SA economy in a material way.
    - The public sector chief audit executives indicated that the role of internal auditing within risk management has mostly evolved in the last year with King II guidance being a major influence. It is concerning that the PFMA, promulgated as it was in 1999 and addressing the role of

internal auditing with regard to risk management, was not mentioned. King III and, to a lesser extent management's and executive management's changed needs, will influence the future involvement of the function.

- Factors influencing the public sector organisations' internal audit functions' involvement in risk management (due to risk immaturity), include the growth in corporate governance guidance, the public's increasing demand for accountability, the function's reputation within the organisation, and internal auditing having an overall understanding of the organisation. Although legislation and financial scandals related to the public sector could have been expected to be indicated as highly influential, these were indicated as a moderate influence.

With reference to the three areas in which internal auditing has duties in managing the risks of the organisation, firstly, internal auditing has responsibilities regarding the risk management framework. The literature study identified, *inter alia*, that internal auditing should provide assurance on the risk management framework, and advise management if the current structures are effective or suitable for the management of risks for the specific organisation. The IIA has provided guidance on these topics, but is lacking detailed guidance on the risk management framework. Additionally, its members do not always adhere to the guidance. Lastly, internal auditors sometimes lack the skills and the knowledge of the business needed to perform these tasks optimally. The empirical study's results are summarised as follows:

- Overall, the chief audit executives indicated that internal audit activities with regard to risk management are performed in line with the IIA guidance.
- The public sector internal auditing functions are performing more consulting services than their private sector counterparts, probably due to internal auditing assisting management with the implementation of a risk management framework as indicated previously. However, this is in contradiction of the chief audit executives' views that internal auditing should not participate in consulting activities with regard to risk

management. The most common factor hindering the public sector's internal audit functions' involvement in risk management is the lack of sufficient resources.

- All the organisations that do have a risk register in place incorporate the results of internal audit engagement findings into this document.
    - The private sector organisations' internal audit functions audit the effectiveness of the methodology followed in the risk management process.
    - With regard to the public sector, internal auditing's involvement is currently very limited.
- It appears that respondents in both the sectors could still be unsure as to which duties the internal audit function are actually performing, or most probably more accurately, are unsure as to how to describe the actions and duties which are performed.

The second area where internal auditing should incorporate risk concepts into its activities is the development of the function's annual plan based on risk. The literature concludes that the audit universe should, *inter alia*, be based on the outcome of the risk management process, especially the strategic risks. The empirical study's results are summarised below:

- All the organisations indicated that the annual plan is based on a risk assessment, incorporating the risks identified by management. However, the loss of opportunity as a risk is not always included.
- Although mostly adhering to the guidance on this topic, public sector organisations do not always adhere to the PFMA guidance. The factor hindering full adherence the most is the lack of resources.

Lastly, internal audit engagements should be risk-based. It appears that limited guidance on this topic is available from the IIA to its members. Internal auditing, in order to continue adding value to the organisation whilst having limited resources in the form of competent internal auditors, and to assist the organisation in meeting its objectives and mitigating its risks, will have to find a new way of performing internal audit engagements. The literature was reviewed

and the steps in the risk management process were compared with the steps of an internal audit engagement planning phase. The outcome supports the use of risk management process methodology to perform internal audit engagements. Based on this, five areas were identified where the current risk-based internal audit engagement planning phase is underdeveloped, namely internal auditors not relying on the risk management process's outcome; the exclusion of loss of opportunities as a form of a risk; the difference between the inherent risk and the residual risk not being used as the starting point of the planning phase; risks not being viewed holistically (that is considering the effect of the risks of this engagement's scope on other areas and other risks affecting this engagement); and controls being mostly used to mitigate the risk while other mitigating forms are not considered. Note that for the rest of this study only private sector organisations' methodologies were obtained. The empirical study's results are summarised as follows:

- Internal auditors mostly base the planning of an internal audit assurance engagement on the methodology of the first COSO model.
- Previous year's working papers as well as inherent risks are used to determine the internal audit engagement plan. The differences between the inherent risks and the residual risks are seldom used as the starting point.
- Although internal auditors rely on the risk register to obtain information for the planning of the internal audit engagement, they also perform their own assessment. Respondents also indicated that they audit the risk management process as well as the outcome of the process. This could be interpreted as internal auditing wasting time on the latter activity, as they do not in any case rely on the outcome when planning an internal audit engagement.
- Engagement planning is based on both threats and loss of opportunities.
- Although respondents indicated that risks are viewed holistically when planning the engagement, only two organisations indicated that the risk management process includes organisation-wide levels. This is further contradicted by respondents indicating that they mainly use the risk register

to identify inherent risks, thus, it can be assumed, excluding organisation-wide risk.

- Respondents also indicated that they prefer to recommend controls as mitigating activities as they feel comfortable doing so. This could lead to over-controlling instead of mitigating a specific risk in the most effective way.

With the above underdeveloped areas in mind, a preliminary model was developed to assist internal auditors when planning a risk-based internal audit engagement. The model can only be used in a risk mature organisation where the risk management process has been properly implemented, has been audited and can be relied upon. The respondents indicated the following:

- The respondents were of the opinion that the model can only benefit the internal audit function's activities including the performance of an internal audit engagement.
- Concerns raised by the respondents varied from aspects outside the direct control of internal auditing, such as that the risk management systems within the organisations are not risk mature, to aspects that internal auditing need to address, such as internal auditors finding it difficult to eliminate over-controlling and over-auditing.
- Respondents were also of the viewpoint that low inherent risks should not be included in the audit, with only one respondent agreeing to a partial inclusion based on the internal auditor's judgment, and one agreeing to inclusion on a surprise basis.
- Where the movement between inherent risk and residual risk was unsatisfactory, the respondents agreed that the internal auditor should focus on the adequacy (and to a lesser extent the effectiveness) of the controls in place to mitigate the risk. One respondent agreed that in such a case an audit finding, without wasting time on testing the controls, is the best solution.

During the third empirical study, the preliminary model was tested at one of the organisations. The planning phase of an audit engagement that was performed previously was re-evaluated, incorporating the methodology of the risk-based internal audit engagement model. The results of the empirical study are summarised below:

- Many of the problems identified by either the literature or by the respondent in the second empirical study, were applicable. These included the fact that the risk register did not distinguish between strategic and operational risks and organisation-wide risks were not identified, the register did not cross-reference to the operational process, and the risk assessment methodologies were limited.
- The results indicate that the use of the model will ensure that fewer audit procedures will be performed, that all the relevant audit findings that would have been included in the audit report will still be identified, and that further aspects could be identified that should be brought to management's attention, either in the audit report as formal audit findings or through interim discussions with management.

Lastly, the preliminary model was refined using the views of the chief audit executives of the five top risk mature organisations obtained in the second empirical study, as well as the results of the testing of the model as per the third empirical study. The adjustments to the model can be summarised as follows:

- Internal auditors need to ensure that the fourth generation internal audit engagement methodology (such as the COSO II model) is followed.
- Internal auditors need to audit the risk management process and, if it is effective, then the outcome as documented in the risk register should be used as the basis of planning the internal audit engagement. Only if no process exists, or if the process is ineffective should the internal auditor perform a risk assessment.
- The internal auditor must include threats and loss of opportunities as risks. In addition, risks in other areas impinging on the audit area must be

included in the audit scope, and risks identified in the current engagement must be integrated into future internal audit engagements.

- Other risk mitigation activities should be considered, not only controls. Management should be made aware of over-controlling, such as instances where the inherent risk is already low but controls still exist.
- The internal auditor must not automatically audit the controls for low inherent risks but, if professional judgement calls for assessing these, should consider performing a surprise check.
- The controls of high residual risk must be investigated for effectiveness only.
- The internal auditor must bring high residual risks to management's attention, either in the audit report as an audit finding, or through discussions with management.

The next section will focus on recommendations that should be taken into consideration by various parties based on the results of the literature study and the three empirical studies. Firstly, to the board and various management levels on the risk management and internal auditing structures and activities within organisations; secondly, to risk management structures on their duties; thirdly, to chief audit executives on the structure of and activities performed by their internal audit functions, specifically their role with regard to risk management; fourthly, to internal auditors on the performance of a risk-based internal audit engagement; and lastly, to the IIA on the guidance provided on risk management and adherence by their members.

6.6 RECOMMENDATIONS

The results of the literature study and the three empirical studies have given rise to certain suggestions that should be taken into consideration by various parties. These recommendations focus specifically on the implementation of risk management within an organisation, the role internal auditing should play in providing assurance, and, lastly, how risk should be incorporated into the internal audit function's activities, specifically the performance of a risk-based internal audit engagement, is provided.

6.6.1 The board and management

Due to the difference in the risk management and internal audit activities within the private and the public sectors, recommendations are made that are applicable to both sectors as well as to each separately.

6.6.1.1 All organisations

- A separate board audit committee and board risk committee is the ideal for the effective management of risk. The risk committee (with the assistance of the risk department and chief risk officer) should focus on the management of risk. The audit committee (with the assistance of the internal audit function and the chief audit executive) should provide assurance on whether risks are managed properly.
- The communication between the applicable board committee(s), risk management structures and internal auditing in respect of the management of risk should be in place and should be effective.
- The effect of the current financial crisis on SA organisations is underestimated, especially with reference to the management of risks. Organisations should bear this in mind.

6.6.1.2 Private sector organisations

- Although most organisations seem to be risk mature, management's lack of commitment to risk management could be a hindering factor for a higher risk maturity level. Two specific areas of concern are the organisational culture of the organisation not supporting risk management, and staff that are not equipped to assist with the management of risks. Management should take steps to rectify these deficiencies.
- The internal audit function should report administratively to the highest possible level within the organisation. Chief audit executives reporting to the chief financial officer and/or the internal audit function being part of the

financial section of the organisation could jeopardise the independence of the function.

6.6.1.3 Public sector organisations

- None of the organisations scored was risk mature. However, the 'internal audit' attribute in the risk maturity model has an above average score. Internal auditing needs to assist management even more in becoming risk mature.
- The composition of the audit committee does not adhere to the King Report requirements – this should be brought in line with the guidance.
- The proper risk management structures are not in place, or the current structures are not sufficient to perform the risk management strategies effectively – this should be addressed.

6.6.2 Risk management structures

Due to the difference in the risk management and internal audit activities within the private and the public sectors, recommendations are made that are applicable to both sectors as well as to each separately.

6.6.2.1 All organisations

- The risk register should be updated on a continuous basis, especially if a risk-specific software programme is used.
- There is a lack of integrated organisation-wide risk management processes (enterprise risk management) that evaluate risks holistically. Risk should not be viewed in silos, but across the whole organisation.
- The risk management processes implemented by management are not risk mature and, therefore, the internal audit function cannot rely on the outcome of the processes. Risk management processes should be implemented and governed better.

- The risk register needs to be structured in such a manner that strategic and operational risks are separated and the latter should be in line with the operational processes.
- The risk assessment methodology should include quantitative analysis, or at minimum include more than just ‘low’, ‘medium’ and ‘high’ measures.

6.6.2.2 Private sector organisations

- The chief risk officer and risk department should report to the highest level within the organisation, for example, the risk committee and an executive management position.

6.6.2.3 Public sector organisations

- The risk management structures are very limited – this should be addressed as a matter of urgency.
- The fact that not one organisation is risk mature should be rectified by the risk management structures.

6.6.3 Chief audit executives

Due to the difference in the risk management and internal audit activities within the private and the public sectors, recommendations are made that are applicable to both sectors as well as to each separately.

6.6.3.1 All organisations

- It appears that chief audit executives are still unsure as to what exactly is expected of internal auditing with regard to the management of risk. It could be that the differences in the terminology and methodology used by organisations, those in the IIA *Standards*, and those used in the literature, are confusing to some individuals. The role of internal auditing regarding risk should be researched and defined.

6.6.3.2 Private sector organisations

- It could be a concerning fact that the internal audit staff has very little internal audit experience. Organisations should assess their internal audit functions and take the necessary steps to ensure the function's success and value adding potential. This includes providing their internal audit staff members with long-term career paths in order to obtain and *keep* competent individuals.

6.6.3.3 Public sector organisations

- Chief audit executives need to be informed of the risk maturity levels of the organisation, and, where applicable, should provide management with advice on how to improve the risk maturity levels.
- The non-adherence to legislation, such as the PFMA, as well as the occurrence of scandals within this sector should encourage the chief audit executives to increase their involvement in the management of risks.
- The non-adherence to the IIA *Standards* on risk-related activities, as well as the limited involvement of the internal audit function in the management of risk, should encourage the use of consultants or experts by the internal audit function.
- The lack of competent internal auditors, resources and risk management knowledge hinders the internal audit function in performing their duties with regard to the management of risks – this should be addressed.

6.6.4 Internal auditors

- The COSO II methodology should be used when performing an internal audit engagement.
- The outcome of the risk management process, as documented in the risk register, should be used to determine the risks threatening the activity under review. If the risk management process's outcome cannot be trusted, internal auditors should perform their own risk assessment to identify high

risk areas. The weaknesses regarding the organisation's risk management process should be reported to management.

- The difference between the inherent risk and residual risk levels should be used as the basis for the planning of an engagement.
- Management should be encouraged to implement risk mitigating activities other than controls. This could lead to eliminating over-controlling.
- Internal auditors should not audit low inherent risk areas, other than where professional judgement urges the internal auditor to, on a surprise basis, inspect a specific area. This could lead to the elimination of over-auditing.
- Areas where the residual risk is still above the risk appetite should at minimum be brought to management's attention, but not be investigated in detail.

6.6.5 Institute of Internal Auditors

- Further guidance is needed for members on how internal auditing could provide assurance on the risk management framework as well as the performance of a risk-based internal audit engagement.
- Although members are of the opinion that they do adhere to the IIA *Standards*, when asked about specific activities with regard to risk management, many of the specific standards, which are compulsory, are not understood and/or adhered to.

6.7 FURTHER RESEARCH

Potential future research studies that have been identified during the course of this study include the following:

- Due to the limited number of responses obtained in the second empirical study, statistical data should be obtained on:
  - the risk management activities within organisations; and
  - the structuring of the internal audit function within the organisation.

- An audit programme or other guidance for internal auditors to use to provide assurance on the risk management framework should be developed.
- The variables that could influence the size of the internal audit function should be investigated.
- The importance of risk management within the corporate governance environment must be clarified, specifically focusing on how internal auditing and external auditing can work together to provide assurance to management on risk management.
- The standing of risk management within the public sector should be investigated and addressed, specially focusing on the concerning fact that chief audit executives, as the assurance providers on risk management within the organisation, are unsure as to whether their organisations are risk mature or not.
- The concept of combined assurance, the various role players, duties and responsibilities, all with specific reference to risk management should be investigated.
- Management's concept and understanding of risk and the management of risk as part of corporate governance – referring both to the knowledge of individuals, potential training, and commitment of the board and senior management should be researched.

6.7 RESEARCH CONCLUSION

In Chapter 1 the research problem was summarised as internal auditors needing to perform internal audit engagements more effectively and efficiently, changing the internal audit methodology to incorporate risk. With limited guidance available from the IIA on this matter it was concluded that the main objective of this study was to develop a risk-based internal audit model to address this gap.

The risk-based internal audit engagement model that was developed divided and addressed risk areas as follows:

- Areas with high operational risks are included in the planning of the internal audit engagement.
- Areas with low risks are only included in the form of a surprise investigation.
- Areas where risks remain high after controls are implemented are not investigated in detail, but rather reported to management on a timely basis.

The use of this model will ensure that internal auditors will focus on the areas that need urgent attention and not waste time on areas that are comparatively insignificant. The effect is that scarce internal audit resources can be allocated to areas where they will add the most value to the organisation.

6.8 FINAL CONCLUSION

Sound corporate governance principles are absolutely essential in the changing environment in which organisations operate, both in the private and the public sectors. Various factors have influenced and still are influencing the need for additional or improved guidance for management on how to manage an organisation more effectively, such as, amongst others, the increase in corporate scandals and stakeholders demanding accountability and transparency. The business environment is trying to address this need by developing more comprehensive and applicable legislation and guidelines. For example, in SA, the three King Reports on Corporate Governance (1994, 2002, 2009) are seen by many as the leading documents in this regard.

The King reports and other such documents are not the only leading publications advocating the concepts of internal auditing and risk management as the cornerstones of sound governance – guidance on what is expected of management in these regards has developed tremendously over the last few decades. With this accelerated evolution of internal auditing and risk management, the question still remains as to why scandals and other collapses, such as the recent global financial crisis, still occur. Why did the risk management implemented by the organisations affected not identify the potential

risks? Where were the auditors in providing assurance on the risk management process and the risk mitigation activities?

This study provides a brief understanding of the risk maturity levels of organisations and the role that internal auditing should play in assisting management in ensuring that the risk management strategy is effectively mitigating risks so that organisational objectives are achieved. It further investigates how internal auditing should adapt their methodologies to incorporate risk into their activities – thus ensuring that the high-risk areas of the organisation are not only identified, but brought to management's attention and then effectively managed. This is in line with the following wise words from internal auditing gurus:

- According to David Landsittel, new chairman of the COSO of the Treadway Commission (cited in Steffee 2009:47):

  > The more companies know about the risks they face, the better. It's also important for companies to be able to identify changes in risk as quickly as possible.

- According to Richard Chambers, chief executive officer of the IIA Inc. (cited in Baker 2010:32):

  > There is pressure on boards to play a stronger role in risk management; they will need someone who is independent and objective to provide them with assurance because they are not going to be there every day and cannot assess all the risks themselves.

- According to Mervyn King, chairman of the King Committee (cited in Baker 2010:31):

  > [The internal auditor] is the ringmaster in combined assurance and the right arm of the non-executive board.

LIST OF REFERENCES

Abdullah, H. & Valentine, B. 2009. Fundamentals and ethics theories of corporate governance. *Middle Eastern Finance & Economics*, Issue 4, pp. 88-96.

Abu-Musa, A.A. 2008. Information technology and its implication for internal auditing. *Managerial Auditing Journal*, Vol. 23, No 5, pp. 438-466.

Addison, S. 2001. Risk and governance issues for ERP enterprise applications. *Information Systems Control Journal,* Vol. 4. [Online] Available from: http://www.isaca.org [Accessed: 8 May 2009].

AGSA: *See* Auditor General.

Ahlawat, S.S., & Lowe, D.J. 2004. An examination of internal auditor objectivity: in-house versus outsourcing. *Auditing: a Journal of Practice and Theory*, Vol. 23, No 2, pp. 147-158.

Alexakis, C.A., Balios, D., Papagelis, G. & Xanthakis, M. 2006. An empirical investigation of the visible effects of corporate governance: the case of Greece. *Managerial Finance*, Vol. 32, No 8, pp. 673-684.

Allegrini, M. & D'Onza, G. 2003. Internal auditing and risk assessment in large Italian companies: an empirical survey. *International Journal of Auditing*, Vol. 7, pp. 191-208.

Allegrini, M., D'Onza, G., Paape, L., Melville, R. & Sarens, G. 2006. The European literature review on internal auditing. *Managerial Auditing Journal,* Vol. 21, No 8, pp. 845-853.

Aluchna, M. 2009. Does good corporate governance matter? Best practice in Poland. *Managerial Research News*, Vol. 32, No 2, pp. 185-198.

Anderson, U. 2003. *Research opportunities in internal auditing - assurance and consulting services.* The Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Anonymous. 2009. The future of the CRO: risk professionals weigh in. *Risk Management*, Vol. 56, No 3, pp. 54-60.

Anonymous. 2004. Parmalat scandal sparks demand for audit experts. *Credit Control,* Vol. 25, No 1, p. 5.

Anonymous. Not dated. *Differences and similarities of the internal auditor versus external auditor.* [Online] Available from: http://accounting-financial-tax.com?2008?08 [Accessed: 6 February 2009].

Apostolou, B., Harper, R.M. & Strawser, J.R. 1990. Reliance on internal audit departments. *Managerial Auditing Journal*, Vol. 5, No 3, pp. 3-9.

Aras, G. & Crowther, D. 2008. Governance and sustainability: an investigation into the relationship between corporate governance and corporate sustainability. *Management Decision*, Vol. 46, No 3, pp. 433-448.

Archibald, R.D. & Lichtenberg, S. 1992. *Experiences using next generation management practices.* Proceedings of the internet world congress on project management, Florence, Italy, Vol.1, pp. 83-97.

Arena, M., Arnaboldi, M. & Azzone, G. 2006. Internal audit in Italian organisations: a multiple case study. *Managerial Auditing Journal*, Vol. 21, No 3, pp. 275-292.

AS/NZS: *See* Australian Standards Board and New Zealand Standards Board.

ASX: *See* Australian Securities Exchange.

Atkins, A. & Webb, A. 2005. *A directors guide to risk and its management.* International Federation of Accountants (IFAC) articles of merit award program for distinguished contribution to management accounting, August.

Atkinson, W. 2008. Board-level risk committees. *Risk Management*, Vol. 55, No 6, pp. 42-45.

Auditor General (AGSA). 2009(a). *National general report of the Auditor General on the audit outcomes of departments, constitutional institutions, public entities and other entities for the financial year 2007-08.* [Online] Available from: http://www.agsa.co.za/Reports%20Documents/General_report_on_the_audit_outcomes_of_departments [Accessed: 17 September 2009].

Auditor General (AGSA). 2009(b). *General report of the Auditor General on the audit outcomes of local government for the financial year 2007-08*. [Online] Available from: http://www.agsa.co.za/Reports%20Documents/General_report_-on_the_audit_outcomes_of_local_government [Accessed: 17 September 2009].

Australian Securities Exchange (ASX) Corporate Governance Council. 2007. *Corporate governance principles and recommendations*. Second edition.

Australian Standards Board and New Zealand Standards Board (AS/NZS). 2004. *Risk Management.* AS/NZS 4360:2004.

Backlund, F. & Hannu, J. 2002. Can we make maintenance decisions on risk analysis results? *Journal of Quality in Maintenance Engineering*, Vol. 8, No 1, pp. 77-91.

Baker, C.B. & Owsen, D.M. 2002. Increasing the role of auditing in corporate governance. *Critical Perspectives on Accounting*, Vol. 13, No 5-6, pp. 783-795.

Baker, N. 2010. Equipped for governance. *Internal auditor*, Vol. 67, No 1, pp. 29-32.

Baker, N.M. 2009. *What is a risk register?* [Online] Available from: http://www.brighthub.com/office/project-managemtny/articles/3247.aspx [Accessed: 29 May 2009].

Baker, N. 2008. Real world ERM. *Internal Auditor,* Vol. 65, No 6, pp. 32-37.

Baker, N. 2005. New hope for Kenya's auditors. *Internal Auditor,* Vol. 62, No 6, pp. 47-50.

Baker, N. 2004(a). Negotiating the rapids. *Internal Auditing and Business Risk*, Vol. 28, No 10, pp. 17-19.

Baker, N. 2004(b). Getting a grip on governance. *Internal Auditing and Business Risk*, Vol. 28, No 3, pp. 14-17.

Balkaran, L. 2008. Two sides to auditing. *Internal Auditor*, Vol. 65, No 5, pp. 22-23.

Bank of Canada. 1998. *Risk-based internal auditing and dynamic control assessment: revolutionising internal audit services.* Institute of Internal Auditors. Altamonte Springs. Florida.

Barac, K. 2008. Verbal communication with senior researcher, UNISA. Pretoria. 22 April 2008.

Barrier, M. 2003. Principles, not rules: thanks to codes drafted under Mervyn King, South Africa has taken the lead in defining corporate governance in broadly inclusive terms*. Internal Auditor*, Vol. 60, No 4, pp. 68-73.

Barton, T.L., Shenkir, W.G. & Walker, P.L. 2008. Managing the unthinkable event. *Financial Executive,* Vol. 24, No 10, pp. 24-29.

Basle Committee. 2004. *Core principles for effective banking supervision.* [Online] Available from: http://www.bis.org/publ/bcbs30a.pdf?noframes=1 [Accessed: 17 February 2009].

Baue, W. 2003. *Johannesburg securities exchange requires compliance with King II and global reporting initiative*. [Online] Available from: http://www.socialfunds.com/news/print.cgi?sfArticleId=1174 [Accessed: 6 February 2009].

Beasley, M.S. 2009. Time to teach ERM. *Internal Auditor*, Vol. 66, No 1, pp. 61-62.

Beasley, M.S., Branson, B.C. & Hancock, B.V. 2009. ERM: opportunities for improvement*. Journal of Accountancy*, Vol. 208, No 3, pp. 28-32.

Beasley, M.S., Branson, B.C. & Hancock, B.V. 2008. Rising expectations*. Journal of Accountancy*, Vol. 205, No 4, pp. 44-51.

Beasley, M.S., Clune, R. & Hermanson, D.R. 2005. Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy,* Vol. 24, Issue 3, pp. 521-531.

Benson, J. 2007. The importance of monitoring. *Internal Auditor*, Vol. 64, No 4, pp. 86-89.

Berley, S. 2007. ERM: time to catch the wave. *Risk Management Magazine*, pp. 22-26.

Bernstein, P.L. 1996. *Against the gods: the remarkable story of risk*. New York: Wiley & Sons.

Bookal, L.E. 2002. Internal auditors: integral to good corporate governance. *Internal Auditor*, Vol. 59, No 4, pp. 44-49.

Borgelt, K. & Falk, I. 2007. The leadership/management conundrum: innovation or risk management? *Leadership and Organisation Development Journal,* Vol. 28, No 2, pp. 122-136.

Bou-Raad, G. 2000. Internal auditors and a value-added approach: the new business regime. *Managerial Auditing Journal*, Vol. 15, No 4, pp. 182-186.

Boyle, T. 2003. Raising the profile of internal audit. *Journal of the Association of Healthcare Internal Auditors.* Winter 2003. [Online] Available from: http://www.acl.com/AHIA _article_winter03.pdf [Accessed: 25 July 2006].

Brannen, L. & Cummings, J. 2005. Fine-tuning internal audit's role. *Business Finance,* Vol. 12, No 12, p. 10.

Breighner, M. 2009. Public sector risk management face unique challenge. *National Underwriter*, Vol. 113, No 21, pp. 20-26.

Brennan, N.M. & Solomon, J. 2008. Corporate governance, accountability and mechanisms of accountability: an overview. *Accounting, Auditing & Accountability Journal*, Vol. 21, No 7, pp. 885-906.

Bridge, S. & Morris, R. 2005. *Saambou bosses face fraud charges*. Business Report. [Online] Available from: http:www.busrep.co.za/general/print_article.php?fArticleId=2876947 [Accessed: 26 August 2009].

Burnaby, P.A., Abdolmohammadi, M., Hass, S., Sarens, G. & Allegrini, M. 2009. Usage of internal auditing standards by companies in the United States and select European countries. *Managerial Auditing Journal*, Vol. 24, No 9, pp. 835-860.

Business Dictionary. 2007/8. *Business risk definition*. [Online] Available from: http://www.businessdictionary.com/definition/business-risk.html [Accessed: 4 June 2008].

Business Times. Not dated. *Companies diligently tow the King line but fail the global test.* [Online] Available from: http://www.btime.co.za/98/1004/comp/comp07.htm [Accessed: 12 February 2009].

CACG: *See* Commonwealth Association for Corporate Governance.

Cadbury Report, A. 1992. *Report of the committee on the financial aspects of corporate governance.* The Committee on the Financial Aspects of Corporate Governance. Gee and Company Limited. London.

Campbell, A. 2009. Job market still poor for risk professionals. *Risk*, Vol. 22, Issue 4, p. 12.

Campbell, M., Adams, G.W., Campbell, D.R. & Rose, M. 2006. Internal audit can deliver more value. *Financial Executive*, Vol. 22, No 1, pp. 44-47.

Campbell, T. 2008. Risk management: implementing an effective system. *Accountancy Ireland*, Vol. 40, No 6, pp. 54-57.

Canada. Treasury Board of Canada Secretariat. 2001. *Integrated risk management framework.* [Online] Available from: http://www.tbs.sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf_cgr_e.asp [Accessed: 6 December 2006].

Carhill, K.M. & Kincaid, J.K. 1989. Applying the standards in governmental internal auditing. *Internal Auditor,* Vol. 46, No 5, pp. 50-55.

Carcello, J.V., Hermanson, D.R., & Raghunandan, K. 2005. Factors associated with U.S. public companies' investment in internal auditing. *Accounting Horizons*, Vol. 19, No 2, pp. 69-84.

Carey, P., Subramaniam, N., & Chua Wee Ching, K. 2006. Internal audit outsourcing in Australia. *Accounting and Finance*, Vol. 46, No 1, pp. 11-30.

Castanheira, N. Rodrigues, L.L. & Craig, R. 2010. Factors associated with the adoption of risk-based internal auditing. *Managerial Auditing Journal,* Vol. 25, No 1, pp. 79-98.

Cenker, W.J. & Nagy, A.L. 2004. Do audit charters need a reality check? *Strategic Finance*, Vol. 85, No 7, pp. 49-53.

Chambers, A. 2008. The board's black hole – filling their assurance vacuum: can internal audit rise to the challenge? *Measuring Business Excellence*, Vol. 12, No 1, pp. 47-63.

Chapman, C. 2004. On the road of change. *Internal Auditor*, Vol. 61, No 3, pp. 40-47.

Chapman, R. 2009. *Maturity models as a vehicle for improving risk management practices.* [Online] Available from: http://blogs.exaprotect.com/2007/09/maturity-models-as-a-vehicle-for-improving-risk [Accessed: 29 May 2009].

Charnock, E. 2009. Holistic compliance: the future of financial risk management. *Financial Executive,* Vol. 25, No 3, pp. 55-57.

Christopher, J., Sarens, G. & Leung, P. 2009. A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting, Auditing & Accountability Journal,* Vol. 22, No 2, pp. 200-220.

Clayton, D. 2009. A risk-centric approach that works. *Internal Auditor*, Vol. 66, No 1, pp. 35-39.

Clemmons, D. 2009. Internal auditors need broader focus and skills. *Internal Auditor*, Vol. 66, No 1, pp. 13-14.

Coetzee, G.P., Du Bruyn, R. & Plant, K. 2007. *Internal auditing: an introduction*. RLP Audit Consultants. Pretoria.

Cole, G.A. 2004. *Management theory and practice.* Sixth edition. London: Continuum.

Committee of Sponsoring Organisations of the Treadway Commission (COSO). 2009. *Strengthening enterprise risk management for strategic advantage.* Sponsoring Organisations of the Treadway Commission. Jersey City. New Jersey.

Committee of Sponsoring Organisations of the Treadway Commission (COSO). 2004. *Enterprise risk management integrated framework: executive summary.* Sponsoring Organisations of the Treadway Commission. Jersey City. New Jersey.

Committee of Sponsoring Organisations of the Treadway Commission (COSO). 1992. *Internal control – integrated framework: framework.* Sponsoring Organisations of the Treadway Commission. Jersey City. New Jersey.

Commonwealth Association for Corporate Governance (CACG). 1999. *Principles for corporate governance in the commonwealth.* [Online] Available from: http://www.ecgi.org/codes/code.php?codeid+2 [Accessed: 31 July 2006].

Continuity Central. 2008. ERM improves decision making and reduces risk. *Business Continuity Journal.* [Online] Available from: http://www.continuity-central.com/news040101.htm [Accessed: 29 May 2009].

Cooper, C. 2008. *Extraordinary circumstances: the journey of a corporate whistleblower*. New Jersey: Wiley & Sons.

Corbin, D. 2005. A cautious perspective on the role of the internal audit function. *IA Advisor*, December, pp. 28-33. Institute of Internal Auditors (SA). Johannesburg.

Corporate Governance Committee. 2003. *The Dutch corporate governance code: principles of good corporate governance and best practice provisions.* Tabaksblat. December.

COSO: *See* Committee of Sponsoring Organisations of the Treadway Commission.

Coupland, D. 1993. The internal auditor's role in public service orientation. *Managerial Auditing Journal,* Vol. 8, No 1, pp. 3-13.

Crawford, M. & Stein, W. 2004. Risk management in UK local authorities: the effectiveness of current guidance and practice. *The international Journal of Public Sector Management*, Vol. 17, No 6, pp. 498-512.

Crowe Chizek. 2006. *Audit committee: 10 ways to collaborate with internal audit.* [Online] Available from: http://www.crowechizek.com/crowe/publications/detail.cfm?id=241 [Accessed: 31 July 2006].

Crowe Chizek. 2005. *Internal audit plays pivotal role in strengthening corporate governance*. [Online] Available from: http://www.crowechizek.com/crowe/publications/detail.cfm?id=149 [Accessed: 31 July 2006].

Curristine, T. 2005. Governance performance: lessons and challenges. *OECD Journal on Budgeting*, Vol. 5, No 1, pp. 127-151.

Curtis, E. & Turley, S. 2006. The business risk audit - a longitudinal case study of an audit engagement*. Accounting, Organizations and Society.* [Online] Available from: http:www.sciencedirect.com/science?_ob=Article [Accessed: 4 December 2006].

Dallas, G. 2004. *Governance and risk: an analytical handbook for investors, managers, directors and stakeholders*. New York: McGraw-Hill.

De Castro, S. 2005. *Corporate governance: new career opportunities*. Lecture at the IOK 711 class, University of Pretoria, August 2005.

De Jager, H. 2009. Verbal communication with senior researcher and public sector specialist, University of Pretoria. Pretoria. 2 September 2009 and 15 October 2009.

De Jager, H. 2008. Verbal communication with senior researcher and public sector specialist, University of Pretoria. Pretoria. 23 April 2008.

De la Rosa, S. 2008(a). Verbal communication with risk consultant, IQ Business Group. Johannesburg. 23 April 2008.

De la Rosa, S. 2008(b). *How to effectively review your organisation's risk management process.* Institute of Internal Auditors Training Program, Johannesburg.

De la Rosa, S. 2007/8. Keeping ERM on the executive's agenda. *Accountancy SA*, December 2007/January 2008, pp. 22-23.

De la Rosa, S. 2007. Taking a closer look at the role of chief risk officer. *IA Advisor*, March. Institute of Internal Auditors (SA). Johannesburg.

Deloitte. 2009. *King III – September 2009 – Every decision counts*. [Online] Available from: https://taxmanagementconsulting.deloitte.co.za/content/1590-/home/# [Accessed: 15 September 2009].

Deloitte. 2005*. Lean and balanced: how to cut costs without compromising compliance*. [Online] Available from: http://www.deloitte.com/dt/research/0,1015, Sid%253D7108%2526cid%253D158271,00.html [Accessed: 17 April 2008].

Deloitte & IIA (UK and Ireland). 2008. *Towards a blueprint for the internal audit profession.* The Institute of Internal Auditors (UK and Ireland). [E-mail to:] Louw, A. (ane.louw@up.ac.za). 10 September 2008.

Deloitte & IIA (UK and Ireland). 2003. *The value agenda.* The Institute of Internal Auditors (UK and Ireland). [E-mail to:] Louw, A. (ane.louw@up.ac.za). 10 September 2008.

De Zoort, F.T., Hermanson, D.R. & Houston, R.W. 2003. Audit committee support for auditors: the effects of materiality justification and accounting precision. *Journal of Accounting and Public Policy*, Vol. 22, pp. 175-199.

Dierks, P.A. & Davis, E.A. 1980. The cruciality and mystique of internal auditing: last prerequisites for professionalism? *Internal Auditor,* Vol. 27, No 2, pp. 36-46.

Dimma, W.A. 2006. *Tougher boards for tougher times: corporate governance in the post-Enron era.* Mississauga, Ont.: Wiley & Sons.

Dittenhofer, M. 2001(a). Reengineering the internal auditing organization. *Managerial Auditing Journal,* Vol. 16, No 8, pp. 458-468.

Dittenhofer, M. 2001(b). Analytical auditing and risk analysis in government. *Managerial Auditing Journal,* Vol. 16, No 8, pp. 469-476.

Dixon, G. & Goodall, G. 2007. The quality assurance review: is your internal audit function effective? *Internal Auditing*, Vol. 22, No 2, pp. 3-6.

Donker, H. & Zahir, S. 2008. Towards an impartial and effective corporate governance rating system. *Corporate Governance*, Vol. 8, No 1, pp. 83-93.

Drew, S.A., Kelley, P.C. & Kendrick, T. 2006. CLASS: five elements of corporate governance to manage strategic risk. *Business Horizons,* Vol. 49, Issue 2, pp. 127-138.

Du Bruyn, R. 2008. Verbal communication with senior lecturer, University of Pretoria. Pretoria. 16 April 2008.

Dunn, J. 1996. *Auditing theory and practice*. Second edition. London: Prentice Hall.

Du Plessis, J. 2009(a). Verbal communication with senior practitioner and specialist in risk management, AURCO. Pretoria. 18 September 2009.

Du Plessis, Y. (Yvonne.duplessis@up.ac.za). 2009(b). Discussion with expert on using the word organisation. [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 12 May 2009.

Du Plessis, J. 2008. Verbal communication with senior practitioner and specialist in risk management, AURCO. Pretoria. 14 March 2008.

Du Preez, V. 2009. Verbal communication with the CEO of the IIA (SA). Johannesburg. 13 May 2009.

Du Preez, V. 2008. Telephonic communication with the CEO of the IIA (SA). Pretoria. 15 April 2008.

Du Toit, D., Knipe, A., Van Niekerk, D., Van der Waldt, G. & Doyle, M. 2002. *Service excellence in governance*. Sandown: Heinemann.

Eccles, N.S., Pillay, V. & De Jongh, D. 2009. Correlates of corporate accountability among South Africa's largest listed companies. *Southern African Business Review*, Vol. 13, No 1, pp. 21-38.

ECGI: *See* European Corporate Governance Institute.

ECIIA: *See* European Confederation of Institutes of Internal Auditing.

Eckhart, K.S., Widener, S.K. & Johnson, L.E. 2001. Governance and local government. *Internal Auditor*, Vol. 58, No 3, pp. 51-55.

Eilifsen, A., Knechel, W.R. & Wallage, P. 2001. Application of the business risk audit model: a field study. *American Accounting Association*, Vol. 15, No 3, pp. 193-207.

Ellingson, J. 2009. Managing risk within a cultural perspective. *Risk Management*, Vol. 56, No 10, pp. 50-53.

Ellis, D. 2008. *US bank giant Lehman to file for bankruptcy*. [Online] Available from: http://edition.cnn.com/2008/business/09/15/lehman.bankruptcy/index.html [Accessed: 26 August 2009].

Elson, R.J. & Lynn, M. 2008. The impact and effect of the Sarbanes Oxley Act on the internal audit profession: chief audit executives' perspectives. *Academy of Accounting and Financial Studies*, Vol. 12, No 1, pp. 59-65.

Emblemsvag, J. & Kjolstad, L.E. 2006. Qualitative risk analysis: some problems and remedies. *Management Decision*, Vol. 44, No 3, pp. 395-408.

Emblemsvag, J. & Kjolstad, L.E. 2002. Strategic risk analysis: a field version. *Management Decision*, Vol. 40, No 9, pp. 842-852.

Erasmus, S. 2009. (Stephanie@iiasa.org.za). 2009. Discussion of membership statistics. [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 17 February 2009.

Erasmus, S. 2008. Verbal communication with membership consultant, IIA (SA). Johannesburg. 9 September 2008.

Ernst & Young. 2009(a). *Business risk report.* [Online] Available from: http://www.ey.com/Global/assets.nsf/International/2009_business_risk_reprot?$file?2009_business_risk_report.pdf [Accessed: 27 March 2009].

Ernst & Young. 2009(b). *Global megatrends*. [Online] Available from: http://www.ey.com/GL/en/Issues/Business-environment/Globl-megatrents-2009 [Accessed: 20 May 2009].

Ernst & Young. 2009(c). *The final King III synopsis*. [Online] Available from: http://www.ey.com/Publications/vwLUAssets/Final_King_III_synopsis/$FILE/090901%20King%20Brochure%20Web.pdf [accessed: 15 September 2009].

Ernst & Young. 2008. *Escalating the role of internal audit: global internal audit survey*. [Online] Available from: http://www.ey.com/Global/assets.nsf/Australia-/AABS_GIAS_2008/$file/GIAS-08.pdf [Accessed: 27 March 2009].

Ernst & Young. 2007. *Global internal audit survey: a current state analysis with insights into future trends and leading practices*. [Online] Available from: http://www.ey.com/Publication/vwLUAssets/Global_Internal_Audit_Survey_conducted_by_Ernst___Young/$FILE/EY_BRS_GlobalInternalAudit07.pdf [Accessed: 21 April 2008].

Ernst & Young. 2006. *Managing risk: stakeholder perspectives*. [Online] Available from: http://www.ey.com/Publication/vwLUAssets/Managing_Risk_Stakeholder_-Perspective/$1FILE/EY_ManagRisk_Stakeholders_Nov06print.pdf [Accessed 20 May 2009].

European Confederation of Institutes of Internal Auditing (ECIIA). 2005. *Internal auditing in Europe*: *position paper*. Brussels. Belgium.

European Corporate Governance Institute (ECGI). Not dated. *Index of codes.* [Online] Available from: http://www.ecgi.org/codes/all_codes.php [Accessed: 9 April 2008].

Fadzil, F.H., Haron, H. & Jantan, M. 2005. Internal auditing practices and internal control system. *Managerial Auditing Journal*, Vol. 20, No 8, pp. 844-866.

Fama, E. & Jensen, M. 1983. Separation of ownership and control. *Journal of Law and Economics*, Vol. 26, pp. 301-325.

Fasset: *See* Finance, Accounting, Management Consulting and other Financial Services.

Faure, G. & De Villiers, C.J. 2004. Employee-related disclosures in corporate annual reports and the King II report recommendations. *Meditari Accountancy Research*, Vol. 12, No 1, pp. 61-75.

Feinstein, A. 2007. *After the party: a personal and political journey inside the ANC*. Johannesburg: Jonathan Ball.

Figg, J. 2000. Outsourcing – a runaway train. *Internal Auditor*, Vol. 57, No 3, pp. 48-55.

Filipek, R. 2007. XBRL comes of age. *Internal Auditor*, Vol. 64, No 5, pp. 29-33.

Finance, Accounting, Management Consulting and other Financial Services (Fasset) Sector Education & Training Authority (SETA). 2007/8. *Scarce skills in the Fasset sector*. [Online] Available from: http://www.fasset.org.za-/downloads/research/Fasset_Scarce_skills_guide2008vs2.doc [Accessed: 17 September 2009].

Financial Reporting Council (FRC). 2005. *Internal control: revised guidance for directors on the combined code*. October.

Flesher, D.L. 1996. *Internal auditing standards and practices*. Institute of Internal Auditors. Altamonte Springs. Florida.

Flint, D. 1988. *Philosophy and principles of auditing: an introduction*. London: MacMillan Education.

Fogarty, T.J. & Kalbers, L.P. 2000. An empirical evaluation of the interpersonal and organisational correlates of professionalism in internal auditing. *Accounting and Business Research,* Vol. 39, No 2, pp. 125-136.

Fourie, H. 2009. Verbal communication with senior lecturer, Tshwane University of Technology. Pretoria. 2 September 2009.

Fourie, H. 2008. Verbal communication with senior lecturer, Nelson Mandela Metropolitan University. Pretoria. 17 April 2008.

Fraser, I. & Henry, W. 2007. Embedding risk management: structures and approaches. *Managerial Auditing Journal*, Vol. 22, No 4, pp. 392-409.

Fraser-Moleketi, G. 2008*. Keynote address at the South African chapter of the association of certified fraud examiners.* [Online] Available from: http://www.info.gov.za/speeches/2008/08091914151001.htm [Accessed: 23 March 2009].

FRC: *See* Financial Reporting Council.

Galloway, D. & Funston, R. Not dated. The challenges of enterprise risk management. *Balance Sheet,* Vol. 8, No 6, pp. 22-25.

Gavin, T.A. & Matherly, C.M. 1997. Outsourcing: An operational auditing perspective. *Managerial Auditing Journal*, Vol. 12, No 3, pp. 116-122.

Gendron, Y., Cooper, D.J. & Townley, B. 2007. The construction of auditing expertise in measuring government performance. *Accounting, Organisations and Society,* Vol. 32, Issue 1-2, pp. 105-133.

Gloeck, J.D. 2005/6. Corporate governance: light years behind accountability. *Auditing SA*, Summer 2005/6, pp. 15-19. South African Institute of Government Auditors.

Gloeck, J.D. & De Jager, H. 1993. *The audit expectation gap in the Republic of South Africa.* School of Accountancy Research Series. Research Report 93(1). University of Pretoria.

Goodwin, J. 2004. A comparison of internal audit in the private and public sectors. *Managerial Auditing Journal*, Vol. 19, No 5, pp. 640-650.

Goodwin-Stewart, J. & Kent, P. 2006(a). Relationship between external audit fees, audit committee characteristics and internal audit. *Journal of Accounting and Finance,* Vol. 46, No 4, pp. 387-404.

Goodwin-Stewart, J. & Kent, P. 2006(b). The use of internal audit by Australian companies. *Managerial Auditing Journal,* Vol. 21, No 1, pp. 81-101.

Gramling, A.A. 1999. External auditors' reliance on work performed by internal auditors: the influence of fee pressure on this reliance decision. *Auditing: a Journal of Practice and Theory*, Vol. 18, pp. 117-143.

Gramling, A.A., Maletta, M.J., Schneider, A. & Church, B.K. 2004. The role of the internal audit function in corporate governance: a synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature*, Vol. 23, pp. 192-244.

Gramling, A.A. & Myers, P.M. 2006. Internal auditing's role in ERM. *Internal Auditor*, Vol. 63, No 2, pp. 52-58.

Grant Thornton. 2010. *Grant Thornton international business report.* [Online] Available from: http://www.grantthorntonibos.com [Accessed: 1 February 2010].

Grant, R.W. & Keohane, R.O. 2005. Accountability and abuses of power in world politics. *American Political Science Review,* Vol. 99, pp. 29-43.

Gray, G.L. 2004. *Changing internal audit practices in the new paradigm: the Sarbanes-Oxley environment.* The Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Green, S. & Gregory, H.J. 2005. The ripple effect. *Internal Auditor*, Vol. 62, No 1, pp. 48-60.

Griffiths, D. 2006(a). *Risk-based internal auditing: an introduction*, 15/03/2006, Version 2.0.3. [Online] Available from: http://www.internalaudit.biz/supporting-pages/resources.htm [Accessed: 20 February 2008].

Griffiths, D. 2006(b). *Risk-based internal auditing: three views on implementation*, 15/03/2006, Version 1.0.1. [Online] Available from: http://www.internalaudit.biz/ sup-porting-pages/resources.htm [Accessed: 20 February 2008].

Griggs, M.D. 2008. The relationship between enterprise risk management and operational risk management*. The RMA Journal,* Vol. 90, No 9, pp. 44-49.

Guner, M.F. 2008. Stakeholders' perceptions and expectations and the evolving role of internal audit*. Internal Auditing*, Vol. 23, No 5, pp. 21-33.

Hahn, R.M. & Kleiner, B.H. 2002. Managing human behaviour in city government. *Management Research News*, Vol. 25, No 3, pp. 1-10.

Halachmi, A. 2005. Governance and risk management: challenges and public productivity. *International Journal of Public Sector Management,* Vol. 18, No 4, pp. 300-317.

Handy, C. 1999. *Beyond certainty: the changing worlds of organisations.* Boston: Harvard Business School Press.

Haron, H., Chambers, A., Ramsi, R. & Ismail, I. 2004. The reliance of external auditors on internal auditors. *Managerial Auditing Journal*, Vol. 19, No 9, pp. 1148-1159.

Harrington, C. 2004. Internal audit's new role. *Journal of Accountancy.* [Online] Available from: http://www.journalof accountancy.com/Issues/2004/Sep/InternalAuditSNewRole [Accessed: 19 March 2009].

Harrington, J. 2008. A barometer for stormy times. *Internal Auditor*, Vol. 65, No 5, pp. 44-51.

Hepworth, N. 2004. *Is the modern risk-based approach to public sector internal audit really appropriate for countries with less developed systems and less well trained public officials?* [Online] Available from: http://www.cipfa.org.uk/international/download/paper.internalaudit_hepworth-oct04.pdf [Accessed: 12 November 2005].

Heracleous, L. 2001. What is the impact of corporate governance on organisational performance? *Corporate Governance*, Vol. 9, No 3, pp. 165-173.

Hermanson, D.R. 2004. Corporate governance ratings: good or bad? *Internal Auditing*, Vol. 19, No 5, pp. 37-40.

Hermanson, D.R. & Rittenberg, L.E. 2003. *Research opportunities in internal auditing – internal audit and organizational governance.* The Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Hespenheide, E. & Funston, R. 2006. The risk-intelligent internal auditor. *Internal Auditing*, Vol. 21, No 2, pp. 12-18.

Hespenheide, E., Pundmann, S. & Corcoran, M. 2007. Risk intelligence: internal auditing in a world of risk. *Internal Auditing,* Vol. 22, No 4, pp. 3-10.

Hettinger, T. 2009. Today's CRO: the role, the fit, the purpose. *Risk Management*, Vol. 56, No 3, pp. 49-52.

Higson-Smith, C. 2000. *Writing your proposal*. [Online] Available from: http://www.nrf.ac.za/yenza/research/proposal.htm [Accessed: 7 November 2002].

Hillson, D.A. 1997. Towards a risk maturity model. *International Journal of Project and Business Risk Management,* Vol. 1, Spring, pp. 35-45.

Hodge, N. 2004. Directors under pressure. *Internal Auditing & Business Risk*, April, pp. 14-18.

Hofmann, M.A. 2009. Interest in enterprise risk management is growing. *Business Insurance*, Vol. 43, No 8, pp. 14-16.

Hofmann, M.A. 2008. Public sector faces unique enterprise risk management challenges. *Business Insurance*, Vol. 42, No 14, pp. 15-16.

Hollyman, G. 2006. *Identifying and auditing non-typical risks using HIV as an example.* Lecture at the IOK 725 class, University of Pretoria, 19 October 2006.

Holt, T.P. & De Zoort, T. 2009. The effects of internal audit report disclosure on investor confidence and investment decisions*. International Journal of Auditing*, Vol. 13, pp. 61-77.

Hopkinson, M. 2004. *Measuring risk management maturity in UK MoD projects*. [Online] Available from: http://www.theirm.org/events/documents/2004-02-05_hopkinson.pdf [Accessed: 29 May 2009].

Houck, T.P. 2003. *Why and how audits must change*. New Jersey: Wiley & Sons.

Hughes, P. 2004. Why auditors audit? *CPA Journal*. [Online] Available from: http://www.nysscpa.org/cpajournal/2004/204/perspectives/nv5.htm [Accessed: 23 March 2009].

Hull, J.C. 2009. The credit crunch of 2007: what went wrong? Why? What lessons can be learned? *The Journal of Credit Risk*, Vol. 5, No 2, pp. 3-18.

Hyde, G. 2007. Enhanced audit testing*. Internal Auditor,* Vol. 64, No 4, pp. 65-68.

IACCM: *See* International Association for Contract & Commercial Management.

IFAC: *See* International Federation of Accountants.

IIA: *See* Institute of Internal Auditors.

iKUTU: *See* Institute of Internal Auditors (IIA) (South Africa), KPMG, University of Pretoria, Tshwane University of Technology, University of South Africa.

Institute of Directors (IOD). 2009*. King report on governance for South Africa.* King Committee on Corporate Governance, Johannesburg.

Institute of Directors (IOD). 2002*. King report on corporate governance for South Africa.* King Committee on Corporate Governance, Johannesburg.

Institute of Directors (IOD). 1994. *King report on corporate governance for South Africa.* King Committee on Corporate Governance, Johannesburg.

Institute of Internal Auditors (IIA), The. 2010. *PA 2200-2: Using a top-down, risk-based approach to identify the controls to be assessed in an internal audit engagement.* [Online] Available from: http://:www.theiia.org/guidance/standards-and-guidance/ippf/practice-advisories/list [Accessed: 23 July 2010].

Institute of Internal Auditors (IIA), The. 2009(a). *International professional practices framework.* Institute of Internal Auditors. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA), The. 2009(b). *IIA position paper: the role of internal auditing in resourcing the internal audit activity*. Institute of Internal Auditors. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA), The. 2009(c). A global perspective on risk. *Tone at the Top*, Issue 43, May, pp. 1-3.

Institute of Internal Auditors (IIA), The. (governance@theiia.org). 2009(d). *IIA headquarters 2009 plan and restructuring.* [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 25 March 2009.

Institute of Internal Auditors (IIA), The. 2009(e). *PA 2010-2: Using the risk management process in internal audit planning.* [Online] Available from: http://www.theiia.org/guidance/standards-and-guidance/ippf/practice-advisories [Accessed: 26 August 2009].

Institute of Internal Auditors (IIA), The. 2009(f*). PA 2050-2: Assurance maps*. [Online] Available from: http://www.theiia.org/guidance/standards-and-guidance/ippf/practice-advisories [Accessed: 26 August 2009].

Institute of Internal Auditors (IIA), The. 2008*. The IIA at a glance*. [Online] Available from: http://www.theiia.org/theiia/about-the-institute [Accessed: 9 April 2008].

Institute of Internal Auditors (IIA), The. 2007(a)*. What are the skill sets and staffing needs of an internal audit activity?* [Online] Available from: http://www.theiia.org/theiia/about-the-profession/internal-audit-faqs/?i=1087 [Accessed: 20 March 2009].

Institute of Internal Auditors (IIA), The. 2007(b). *GAIN: Global audit information network.* [Online] Available from: http://www.theiia.org/guidance/benchmarking/2007_Sample_Reprot[1].pdf [Accessed: 19 November 2009].

Institute of Internal Auditors (IIA), The. 2006(a). *New guidance for the professional practices framework.* Revised version 9/2/2006. Institute of Internal Auditors. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA), The. 2006(b). *IIA position paper on organisational governance: guidance to internal auditors.* [Online] Available from: http://www.theiia.org/guidance/additional-resources/suppressed-pdf/?serach=positionpaperorganizationalgovernance [Accessed: 23 March 2009].

Institute of Internal Auditors (IIA), The. 2004. *IIA position statement: the role of internal auditing in enterprise-wide risk management issues*. [Online] Available from: http://www.theiia.org/iia/index.cfm?act=iianews&detail=4910 [Accessed: 12 October 2004].

Institute of Internal Auditors (IIA), The. 1999. *A vision for the future: professional practices framework for internal auditing*. Institute of Internal Auditors. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA), The. Not dated(a). *About the institute of internal auditors*. [Online] Available from: http://www.theiia.org/index.cfm?doc_id=270 [Accessed: 20 April 2005, 9 April 2008, 6 February 2009, 9 February 2009].

Institute of Internal Auditors (IIA), The. Not dated(b). *IIA: 2007 annual report*. [Online] Available from: http://www.theiia.org/newsroom/annual report/search=annual%20report [Accessed: 9 February 2009].

Institute of Internal Auditors (IIA), The. Not dated(c). *Find an IIA institute near you*. [Online] Available from: http://www.theiia.org/chapters/index.cfm?act=all.list [Accessed: 6 February 2009].

Institute of Internal Auditors (IIA), The. Not dated(d). *Certification: candidate handbook.* [Online] Available from: http://www.theiia.org/certification [Accessed: 9 February 2009].

Institute of Internal Auditors (IIA), The. Not dated(e). *Membership in the IIA: get the competitive edge*. [Online] Available from: http://www.theiia.org/membership-/why-join/index.cfm?print [Accessed: 6 February 2009].

Institute of Internal Auditors (IIA), The. Not dated(f). *Competency framework for internal auditors.* [Online] Available from: http://www.theiia.org/guidance/standards-and-practices/additional-resources/competency%20framework. [Accessed: 30 September 2008].

Institute of Internal Auditors (IIA), The. Not dated(g). *Membership net growth*. [Online] Available from: http://www.theiia.org/committees/membership-committee/global-membership-statistics/?search=membership%20statistics [Accessed: 9 June 2009].

Institute of Internal Auditors (IIA), The. Not dated(h). *Advocacy: a common thread.* Institute of Internal Auditors. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA) France. 2005. *Survey risk management and mapping process*. Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA) (New Zealand) & KPMG. 2009. *Independence: an emerging issue for public sector audit committees.* [Online] Available from: http://www.kpmg.co.nz/pages/102812.html [Accessed: 16 March 2009].

Institute of Internal Auditors (IIA) Research Foundation, The. 2009(a). *Knowledge alert: 2009 hot topics for the internal audit profession.* Global Audit Information Network. Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA) Research Foundation, The. 2009(b). *ERM benchmarking survey.* Global Audit Information Network. Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA) Research Foundation, The. 2009(c). *The financial crises and its impact on the internal audit profession.* Global Audit Information Network. Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA) Research Foundation, The. 2009(d). *Internal audit capability model for the public sector*. Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA) Research Foundation, The. 2007. *CBOK (A global summary of the common body of knowledge 2006)*. Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Institute of Internal Auditors (IIA) (South Africa), The. 2008. *IA Advisor*, December. Institute of Internal Auditors (SA). Johannesburg.

Institute of Internal Auditors (IIA) (South Africa), The. Not dated(a). *About the institute of internal auditors: the IIA SA.* [Online] Available from: http://www.iiasa.org.za/navigation.htm [Accessed: 9 September 2008, 9 February 2009].

Institute of Internal Auditors (IIA) (South Africa), The. Not dated(b). *About the institute of internal auditors: membership.* [Online] Available from: http://www.iiasa.org.za/navigation.htm [Accessed: 9 February 2009].

Institute of Internal Auditors (IIA) (South Africa), KPMG, University of Pretoria, Tshwane University of Technology, University of South Africa (iKUTU). 2009*. The standing of and demand for internal auditing in South African companies.* [Online] Available from: http://www.iiasa.org.za/Technical/iKUTU_Research_Report.pdf [Accessed: 12 March 2010].

Institute of Internal Auditors (IIA) (UK and Ireland). 2003. *Position statement: risk based internal auditing.* [Online] Available from: http://www.iia.org.uk [Accessed: 14 March 2007].

Institute of Risk Management (IRM). 2002. *A risk management standard.* [Online] Available from: http://www.theirm.org/publications/Pustandards.html [Accessed: 12 April 2007].

International Association for Contract & Commercial Management (IACCM). 2002. *Organisational maturity in business risk management: the IACCM business risk management maturity model (BRM3).* [Online] Available from: http://www.risk-doctor.com/pdf-files/brm1202.pdf [Accessed: 29 May 2009].

International Federation of Accountants (IFAC). 2004. *Enterprise governance: getting the balance right.* Professional Accountants in Business Committee of the International Federation of Accountants. [Online] Available from: http://www.ifac.org [Accessed: 19 September 2005].

International Federations of Accountants (IFAC). 1994. *Using the work of other auditors – a public sector perspective*. Public Sector Committee. International Federations of Accountants (IFAC). New York.

International Organisation for Standardisation (ISO). 2007. *Risk management – guidelines on principles and implementation of risk management*. ISO 31000. Draft. International Organisation for Standardisation. Geneva.

IOD: *See* Institute of Directors.

IRM: *See* Institute of Risk Management.

ISO: *See* International Organisation for Standardisation.

IT Governance Institute. Not dated. *Cobit 4.1.* [Online] Available from: http://isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/CobiT4.1_Brochure.pdf [Accessed: 9 May 2009].

Jackson, R.A. 2007. The human side of risk. *Internal Auditor*, Vol. 64, No 5, pp. 38-44.

Jackson, R.A. 2005(a). In praise of independent insiders. *Internal Auditor,* Vol. 62, No 3, pp. 68-71.

Jackson, A. 2005(b). Corporate governance update. *Corporate Governance: an International Review*, Vol. 13, No 2, pp. 345-350.

Jackson, R.A. 2004. Principles versus rules. *Internal Auditor*, Vol. 61, No 5, pp. 57-61.

James, K.L. 2004. Structuring internal audit reporting to enhance user confidence*. Internal Auditing*, Vol. 19, No 1, pp. 17-20.

Jayalakshmy, R. Seetharaman, A. & Wei Kong, T. 2005. The changing role of internal auditors. *Managerial Auditing Journal*, Vol. 20, No 3, pp. 249-271.

Johnson, V. 2009. (veronica.johnson@theiia.org). 2009. Discussion of CIA statistics. [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 4 March 2009.

Johri, H.P., Cooper, J.C. & Prokopenko, J. 1998. Managing internal consulting organisation: a new paradigm. *Advanced Management Journal*, Vol. 63, pp. 4-7.

Johri, H.P. & Molnar, J. 1989. Developing an internal consulting group in a large organisation using an institution building approach. *International Journal of Public Sector Management*, Vol. 2, Issue 3, pages not known.

Kalaw, M. 2002. *Global governance, civil society and earth summit 2002.* [Online] Available from: http://www/ncsdnetwork.org/knowledge/global_governance.pdf [Accessed: 6 December 2006].

Keen, S. 2008. *Economics 101 – what the global meltdown means.* [Online] Available from: http://www.theage.com.au?action/printArtile?id=226496 [Accessed: 12 February 2009].

Khoabane, P. 2009. *Niehaus is a wake-up call for corporate South Africa.* The Times, 22 February 2009. [Online] Available from: http://www.thetimes.co.za/ Columnists/News/Article.aspx?id=944066 [Accessed: 23 March 2009].

Killackey, H. 2009. Integrating enterprise risk management with organisational strategy. *The RMA Journal*, Vol. 91, No 8, pp. 28-35.

Kimbrough, R.L. & Componation, P.J. 2009. The relationship between organisational culture and enterprise risk management. *Engineering Management Journal*, Vol. 21, No 2, pp. 18-26.

King, M.E. 2007. *Does good governance add to the market cap of a company?* Paper presented at the International Conference of the Institute of Internal Auditors Inc., Amsterdam, Netherlands, 9 July 2007.

Kleffner, A.E., Lee, R.B. & McGannon, B. 2003. The effect of corporate governance on the use of enterprise risk management: evidence from Canada. *Risk Management and Insurance Review*, Vol. 6, No 1, pp. 53-73.

Knechel, W.R. 2006. The business risk audit: origins, obstacles and opportunities. *Accounting, Organizations and Society*, Vol. 32, Issue 4-5, pp. 383-408.

Koh, H.C. & Woo, E. 1998. The expectation gap in auditing. *Managerial Auditing Journal*, Vol. 13, No 3, p. 147.

Koutoupis, A.G. & Tsamis, A. 2009. Risk based internal auditing within Greek banks: a case study approach. *Journal of Management and Governance*, Vol. 13, Issue 1-2, pp. 101-130.

KPMG. 2008/9. *Integrity survey.* [Online] Available from: http://www.404-institute.com/docs/KPMG_Integrity?Survey_2008-9.pdf [Accessed: 27 March 2009].

KPMG. 2005. *Toolkit for the audit committee*. First edition. KPMG Services (Pty) Ltd. Johannesburg. South Africa.

KPMG. 2003(a). *King II, the KPMG quick reference guide*. KPMG Services (Pty) Ltd. Johannesburg. South Africa.

KPMG. 2003(b). *Internal audit's role in modern corporate governance*. [Online] Available from: http://www.kpmg.com.au/aci/docs/int-audit-role-in-corp-gov.pdf [Accessed: 25 July 2006].

Krell, E. 2006. First-movers step up the pace of governance. *Business Finance,* Vol.12, No 6, pp. 36-40.

Krell, E. 2005. Is Sarbanes-Oxley compromising internal audit? *Business Finance*, Vol. 11, No 8, pp. 18-22.

Krogstad, J.L., Ridley, A.J. & Rittenberg, L.E. 1999. Where we're going? *Internal Auditor*, Vol. 56, No 5, pp. 27-33.

Lacey, M.Y. & Tompkins, T.C. 2007. Analysis of best practices of internal consulting. *Organisational Development Journal,* Vol. 25, No 3, pp. 123-131.

Lam, J. 2009. Key requirements for enterprise-wide risk management: lessons learned from the global financial crisis. *RMA Journal*, Vol. 91, No 8, pp. 22-27.

Lapointe, J. 2004. An audit transformation. *Internal Auditor,* Vol. 61, No 5, pp. 62-66.

Leedy, P.D. & Ormrod, J.E. 2005. *Practical research: planning and design*. Eighth edition. Upper Saddle River, New Jersey: Pearson Education International.

Lemon, W.M. & Tatum, K.W. 2003. *Research opportunities in internal auditing: Internal auditing's systematic and disciplined process.* The Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Lenckus, D. 2009. Demonstration of ERM's usefulness key to winning over management. *Business Insurance*, Vol. 43, No 20, pp. 16-18.

Lenckus, D. 2006. RIMS launches online tool to advance ERM. *Business Insurance*, Vol. 40, No 49, pp. 1-2.

Letza, S., Kirkbride, J., Sun, X. & Smallman, C. 2008. Corporate governance theories: limits, critics and alternatives. *International Journal of Law and Management,* Vol. 50, No 1, pp. 17-32.

Leung, F. & Isaacs, F. 2008. Risk management in public sector research: approach and lessons learned at a national research organisation. *R&D Management,* Vol. 38, No 5, p. 510.

Leung, P., Cooper, B.J. & Robertson, P. 2003. *The role of internal audit in corporate governance and management.* Institute of Internal Auditors (Australia). Institute of Internal Auditors Research Foundation & RMIT University. Melbourne.

Lewis, R. 2007. *Corporate governance: a combined code time-line*. [Online] Available from: http://www.accountingweb.co.uk/cgi-bin/item.cgi?id=174351&d [Accessed: 17 February 2009].

Liebowitz, M. 2007. Taking ERM to the next level. *Risk Management*, Vol. 54, No 3, p. 44.

Loots, J.A.J. 1989. *An evaluation of the applicability of comprehensive auditing in the South African context.* Unpublished DCom (Accounting) thesis. University of Pretoria.

Lubbe, D. 2009. *'Politieke bedrog' dalk 'n rede vir ekonomiese krisis*. Volksblad. [Online] Available from: http://jv.news24.com/Die_Volks-blad/Nuus/0,,5-83_2533291,00.html [Accessed: 20 August 2009].

Lubbe, D. 2008(a). Qualified auditors' reports: what's gone wrong? *Accountancy SA*, June, pp. 28-29.

Lubbe, J. 2008(b). Verbal communication with senior practitioner, Rand Merchant Bank. Johannesburg. 6 June 2008.

Lubbe, J. & Van der Merwe, R. 2007. The relationship between ERM and internal audit. *Accountancy SA*, June, pp. 24-29.

Maher, M. & Akers, M.D. 2003. Internal audit's role in system development: the CEO's perspective. *Internal Auditing*, Vol. 18, No 1, pp. 35-39.

Mallin, C.A. 2007. *Corporate governance.* Second edition. New York: Oxford University Press.

Mantey, N. 2009. The internal auditor's role in IT governance. *Auditing SA*, Summer 2008/9, pp. 41-43.

Mardjono, A. 2005. A tale of corporate governance: lessons why firms fail. *Managerial Auditing Journal*, Vol. 20, No 3, pp. 272-283.

Markham, J.W. 2006. *A financial history of modern US corporate scandals: from Enron to reform*. New York: ME Sharp.

Marks, N. 2008. At the root of risk*. Internal Auditor*, Vol. 65, No 5, pp. 29-31.

Marks, N. 2007. Internal audits of governance. *Internal Auditor*, Vol. 64, No 6, pp. 31-32.

Marks, N. 2001. The new age of internal auditing. *Internal Auditor*, Vol. 58, No 6, pp. 44-49.

Martin, P.H. 2009/10. As risk management evolves, is operational risk management important? *The Journal of Operational Risk*, Vol. 4, No 4, pp. 75-84.

Marx, B. 2008. *An analysis of the development, status and functioning of audit committees at large listed companies in South Africa*. Unpublished DCom (Auditing) thesis. University of Johannesburg.

Massachusetts Institute of Technology (MIT) Center for Transportation & Logistics. Not dated. *A risk maturity model.* [Online] Available from: http://ctl.edu/index.pl?id=11756&isa=Category&op=show_printer_friendly [Accessed: 29 May 2009].

Mathephe, E. 2009. (Ezekiel.Mathephe@fin24.com). Results of McGregor BFA top 40 companies. [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 8 April 2009.

Mathker, V. 2008. *Sub-prime bomb: where were the auditors?* [Online] Available from: http://in.rediff.com/cms/print.jsp?docpath=//money/2008/0ct/15bcrisis.htm [Accessed: 24 March 2009].

Matsi, K. 2009. (KediM@agsa.co.za). Results on the Auditor General's reports. [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 17 September 2009.

Mautz, R.K. & Sharaf, H.A. 1961. The *philosophy of auditing*. American Accounting Association. Menasha. Wisconsin.

Mayhew, B.W., Scatzberg, J.W. & Sevcik, G.R. 2001. The effect of accounting uncertainty and auditor reputation on auditor objectivity. *Auditing: A Journal of Practice & Theory*, September, pp. 49-70.

McCall, S.M. 2002. The auditor as consultant. *Internal Auditor,* Vol. 59, No 6, pp. 35-39.

McCarthy, M.P. & Flynn, T.P. 2004. *Risk: from the CEO and board perspective*. New York: McGraw-Hill.

McCaul, L. 2006(a). Enhancing the value of internal audit: ten key questions. *Accountancy Ireland*, Vol. 38, No 3, pp. 35-37.

McCaul, L. 2006(b). Head of IA: the importance of succession planning. *Accountancy Ireland*, Vol. 38, No 6, pp. 18-21.

McCollum, T. 2009. Rising to the occasion*. Internal Auditor*, Vol. 66, No 1, pp. 47-49.

McCuaig, B. 2006. Considering risk in audit planning*. Internal Auditing*, Vol. 21, No 4, pp. 3-12.

McDonald, C. 2009. Will ERM survive the economic meltdown? *National Underwriter*, Vol. 113, No 15, pp. 27-35.

McDonald, C. 2007. RIMS offers ERM maturity model tool. *National Underwriter*, Vol. 111, No 3, pp. 28-29.

McIntosh, E.R. 1999. *Competency framework for internal auditing: an overview.* The Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

McNamee, D. 1998. *Business risk assessment*. The Institute of Internal Auditors. Altamonte Springs. Florida.

McNamee, D. 1997. Risk-based auditing. *Internal Auditor*, Vol. 54, No 4, pp. 22-27.

McNamee, D. & Selim, G.M. 1999. The next step in risk management. *Internal Auditor*, Vol. 56, No 3, pp. 35-39.

McNamee, D. & Selim, G.M. 1998. *Risk management: changing the internal auditor's paradigm*. Institute of Internal Auditors. Altamonte Springs. Florida.

McPhee, I. 2005. *Risk and risk management in the public sector.* Public sector governance and risk forum held on 1 September 2005. [Online] Available from: http://www.anao.gov.au [Accessed: 14 November 2005].

Meiselman, J. 2007. Risk, governance and compliance trends for 2007. *Risk Management,* Vol. 54, No 2, p. 40.

Meislin, M. 2002. *Internal consultants: three ways to stay at the strategic table*. Consulting Today. [Online] Available from: http://www.marcia-meislin.com/article/by_marcia/Internal-Consultant.pdf [Accessed: 20 May 2009].

Merna, T. & Al-Thani, F.F. 2005. *Corporate risk management: an organisational perspectice*. West Sussex: Wiley & Sons.

Meulbroek, L. 2002. *Integrated risk management for the firm: a senior management's guide*. Boston: Harvard Business School Press.

Mihret, D.G. & Yismaw, A.W. 2007. Internal audit effectiveness: an Ethiopian public sector case study. *Managerial Auditing Journal*, Vol. 22, No 5, pp. 470-484.

Minsky, S. 2009. *New era of risk management*. [Online] Available from: http://www.ebizq.net/blogs/chief_risk_officer/2009/01/evidence_links_erm_directly_to_improved_business_performance [Accessed: 29 May 2009].

MIT: *See* Massachusetts Institute of Technology.

Moeller, R.R. 2002. *Sarbanes-Oxley and the new internal auditing rules*. New Jersey: Wiley & Sons.

Moody, M.J. 2009. ERM: the big picture. *Rough Notes*, Vol. 152, No 1, pp. 74-75.

Moody, M.J. 2007. RIMS' risk maturity model. *Rough Notes,* Vol. 150, No 4, pp. 100-101.

Moody, M.J. 2006. Enterprise risk management: immediate impact by rating agencies*. Rough Notes*, Vol. 149, No 8, pp. 40-41.

MORI Social Research Institute. 2002. *Public attitudes to risk.* Strategy Unit: London.

Morrill, C. & Morrill J. 2003. Internal auditors and the external audit: a transaction cost perspective. *Managerial Auditing Journal*, Vol. 18, No 6/7, pp. 490-504.

Mouton, J. 2001. *How to succeed in your master's & doctoral studies: a South African guide and resource book*. Pretoria: Van Schaiks.

Nagy, A.L. & Cenker, W.J. 2002. An assessment of the newly defined internal audit function. *Managerial Auditing Journal*, Vol. 17, No 3, pp. 130-137.

Newsome, R. 2009. Verbal communication with risk expert and spokesperson for the IIA (SA) on King Report III. 13 May 2009.

Newsome, R. 2004. Corporate governance in SA. *IA Advisor,* July, pp. 26-31. Institute of Internal Auditors (SA). Johannesburg.

New York Stock Exchange (NYSE). 2003. *NYSE corporate governance rules*. [Online] Available from: http://www.nyse.com/pdfs/finalcorpgovrules.pdf [Accessed: 19 March 2009].

Nocco, B.W. & Stulz, R.M. 2006. Enterprise risk management: theory and practice. *Journal of Applied Corporate Finance*, Vol. 18, No 4, pp. 8-20.

NYSE: *See* New York Stock Exchange.

O'Brien, J. 2005. *Governing the corporation*. West Sussex: Wiley & Sons.

OECD: *See* Organisation for Economic Co-operation and Development.

Olah, A.J. 2009. Where was ERM? *Internal Auditor*, Vol. 66, No 1, p. 11.

O'Regan, D. 2001. Genesis of a profession: towards professional status for internal auditing. *Managerial Auditing Journal*, Vol. 16, No 4, pp. 215-226.

Organisation for Economic Co-operation and Development (OECD). 2004. *OECD principles of corporate governance.* [Online] Available from: http://www.oecd.org/dataoecd/32/18/31557724.pdf [Accessed: 6 February 2009].

Organisation for Economic Co-operation and Development (OECD). 1999. *OECD principles of corporate governance*. [Online] Available from: http://www.oecd.org/ [Accessed: 20 April 2005].

Owen, R. 2009. Verbal discussion with statistician, University of Pretoria. Pretoria. 15 September 2009 and 6 October 2009.

Oxford Dictionary. 2005. *South African concise oxford dictionary*. Fourth edition. Cape Town: Oxford University Press.

Oxner, T. & Oxner, K. 2006. Boom time for internal audit professionals. *Internal Auditor*, Vol. 63, No 3, pp. 50-57.

Paape, L. Scheffe, J. & Snoep, P. 2003. The relationship between the internal audit function and corporate governance in the EU: a survey. *International Journal of Auditing*, Vol. 7, pp. 247-262.

Palmer, L.A. 2008. Considering bias in government audit reports. *Journal of Business Communication*, Vol. 45, No 3, pp. 265-285.

Pang, L. 2001. Manager's guide to enterprise resource planning (ERP) systems. *Information System Control Journal*, Vol. 4. [Online] Available from: http://isaca.org [Accessed: 8 May 2009].

Pauw, J.C., Woods, G., Van der Linde, G.J.A., Fourie, D. & Visser, C.B. 2002. *Managing public money: a system from the south*. Sandown: Heinemann.

Pelletier, J. 2008. Adding risk back into the audit process. *Internal Auditor,* Vol. 65, No 4, pp. 73-76.

Peterson, A. Looking for risk in all the right places. *Internal Auditing*, Vol. 21, No 5, pp. 3-16.

Plant, K. 2009. Verbal communication with senior lecturer, University of Pretoria. Pretoria. 9 September 2009.

Porter, B.A. 2009. The audit trinity: the key to securing corporate accountability. *Managerial Auditing Journal*, Vol. 24, No 2, pp. 156-182.

Potok, N. 2009. Addressing the accountability challenge. *Public Manager*, Vol. 38, No 1, pp. 76-82.

PricewaterhouseCoopers (PWC). 2009. *Corporate governance – King III.* [Online] Available from: http://www.pwc.com/za/en/king3/index.jhtml?preview+true [Accessed: 15 September 2009].

PricewaterhouseCoopers (PWC). 2008(a). *Targeting key threats and changing expectations to deliver greater value.* [Online] Available from: http://www.pwc.com/extweb/pwcpublications.nsf/docid/state_internal_audit_profession_study_08.pdf [Accessed: 3 May 2008].

PricewaterhouseCoopers (PWC). 2008(b). *Internal audit 2012: a study examining the future of internal auditing and the potential decline of a controls-centric approach.* [Online] Available from: http://www.pwc.com/images/gx/eng/about/svcs/grms/PwC_IAS_2012.pdf [Accessed: 3 May 2008].

PricewaterhouseCoopers (PWC). 2007. *State of the internal audit profession study: pressures build for continual focus on risk*. [Online] Available from: http://www.pwc.com/extweb/pwzpublications.nsf/StateProfessionStudy2007.pdf [Accessed: 12 March 2008].

PricewaterhouseCoopers (PWC). 2006. *Enterprise risk management benchmarking survey*. [Online] Available from: http://www.pwc.com/fi/fin /about/svcs/neuvonta/Erm_study_2006.pdf [Accessed: 29 May 2009].

PricewaterhouseCoopers (PWC). 1999. *Enhancing shareholder wealth by better managing business risk.* Financial and Management Accounting Committee. International Federation of Accountants. New York.

Prinsloo, J. 2008. *The development and evaluation of risk-based approaches*. Unpublished MCom (Accounting) dissertation. University of the Free State.

PRMIA: *See* Professional Risk Managers' International Association.

Professional Risk Managers' International Association (PRMIA). 2008. *Enterprise risk management: a status check on global best practices.* [Online] Available from: http://www.prmia.org [Accessed: 12 March 2009].

Pryal, M. 2008. A broader array of skills. *Internal Auditor*, Vol. 65, No 3, pp. 39-43.

Psica, A. 2008. The right fit: auditing ERM frameworks. *Internal Auditor,* Vol. 65, No 2, pp. 50-56.

Puccia, M. 2007. *The role of ERM in ratings - Standard & Poor's framework for assessing ERM practices.* [Online] Available from: www. Standardandpoors.com/spf/pdf/products/ICR_Article_CriteriaAssessingEnterpriseRisk.pdf [Accessed: 14 April 2008].

PWC: *See* PricewaterhouseCoopers.

Ramamoorti, S. 2003. *Research opportunities in internal auditing - internal auditing: history, evolution and prospect.* The Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Ramamoorti, S., Watson, M.W. & Zabel, M. 2008. Engineering value into enterprise risk management. *Internal Auditor*, Vol. 65, No 5, pp. 53-59.

Ramamoorti, S. & Weidenmier, M.L. 2003 *Research opportunities in internal auditing: the pervasive impact of information technology on internal auditing.* The Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Reding, K.F., Sobel, P.J., Anderson, U.L., Head, M.J., Ramamoorti, S. & Salamasick, M. 2007. *Internal auditing: assurance and consulting services.* Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Reeve, J.T. 1986. *Cashin's handbook for auditors*. Second edition. Englewood Cliffs. New Jersey: Prentice Hall.

Reinstein, A., Lander, G.H. & Gavin, T.A. 1991. The external auditor's consideration of the internal audit function. *Managerial Auditing Journal*, Vol. 9, No 7, pp. 29-36.

Richardson, B. & Gerzon, P. Not dated. *Emergent risks*. [Online] Available from: http://www.theirm.org/publications/documents/irm_emergent_riks.pdf [Accessed: 4 June 2008].

RIMS: *See* Risk and Insurance Management Society.

Risk and Insurance Management Society (RIMS), Inc. 2006. *RIMS risk maturity model for enterprise risk management.* [Online] Available from: http://www.rims.org/rmm [Accessed: 12 March 2008].

Rittenberg, L.E. & Anderson, R.J. 2006. A strategic player. *Journal of Accountancy,* July, Issue 202:1, pp. 51-54.

Rivenbark, W.C. 2000. Embracing risk-based auditing in local government. *Government Finance Review*, Vol. 16, No 3, pp. 17-20.

Rizzi, J.V. 2008. Rethinking risk management. *Commercial Lending Review*, November/December, pp. 3-8.

Robert Half International. 2008. *Salary guide: accounting and finance*. Robert Half International Inc. Corporate Office. California. USA.

Robert Half International. 2007. The red carpet treatment. *Journal of Accountancy*, August 2007. [Online] Available from: http://www.aicpa.prg/PUBS/ jofa/aug2007/rhi.htm [Accessed: 29 February 2008].

Roffia, P. 2007. *The internal auditing function in Italian listed companies: state of the art and future perspective.* Paper presented at the 5th European Conference on Internal Audit and Corporate Governance, Pisa, 18-20 April, pp. 2-16.

Rose, R. 2003. JSE responsibility index to measure non-financial risks. *Business Day (SA) Limited*, 16 October, p. 17.

Rowe, C.A. 2004. Managing risk in the public sector. *Risk Management Magazine*, Vol. 51, No 11, p. 52.

SA: *See* South Africa.

SAICA: *See* South African Institute of Chartered Accountants.

Sarens, G. & De Beelde, I. 2006(a). Internal auditors' perception about their role in risk management: a comparison between US and Belgian companies. *Managerial Auditing Journal*, Vol. 21, No 1, pp. 63-80.

Sarens, G. & De Beelde, I. 2006(b). The relationship between internal audit and senior management: a qualitative analysis of expectations and perceptions. *International Journal of Auditing*, Vol. 10, pp. 219-241.

Sass, M. 2005. Strategies to enhance internal auditing. *IA Advisor*, December, pp. 13-19. Institute of Internal Auditors (SA). Johannesburg.

Saunders, M., Lewis, P. & Thornhill, A. 2007. *Research methods for business students*. Fourth edition. Essex: Prentice Hall.

Sawyer, L.B., Dittenhofer, M.A. & Scheiner, J.H. 2003. *Sawyer's internal auditing.* Fifth edition. The Institute of Internal Auditors. Altamonte Springs. Florida.

Sawyer, L.B., Dittenhofer, M.A. & Scheiner, J.H. 1996. *Sawyer's internal auditing.* Fourth edition. The Institute of Internal Auditors. Altamonte Springs. Florida.

Schanfield, A. & Helming, D. 2008. Top ERM implementation challenges. *Internal Auditor,* Vol. 65, No 6, pp. 41-44.

Schneider, A. 2008. Outsourcing internal auditing. *Internal Auditing*, Vol. 23, No 6, pp. 16-25.

Selim, G. & Yiannakas, A. 2000. Outsourcing the internal audit function: survey of the UK public and private sectors. *International Journal of Auditing*, Vol. 4, pp. 213-226.

Shenkir, W.G. & Walker, P.L. 2006. Enterprise risk management and the strategy risk focused organisation. *Cost Management*, Vol. 20, No 3, pp. 32-38.

Sherer, M. & Kent, D. 1983. *Auditing and accountability*. London: Pitman Books.

Sidani, Y.M. 2007. The audit expectation gap: evidence form Lebanon. *Managerial Auditing Journal*, Vol. 22, No 3, pp. 288-302.

Siegel, P.H. & O'Shaughnessy, J. 2008. Social skill characteristics that promote successful careers in internal auditing. *Internal Auditing*, Vol. 23, No 1, pp. 26-32.

Singer, S.H. 2008. The evolving internal audit people model. *Internal Auditing*, Vol. 23, No 1, pp. 3-11.

Singh, C. 2010. Telephonic communication with the internal audit function at the South African Revenue Services (SARS) regarding communication policy. Pretoria. 15 April 2008.

Singh, H. & Newby, R. 2010. Internal audit fees: further evidence. *Managerial Auditing Journal,* Vol. 25, No 4, pp. 309-327.

Skipper, H.D. 1998. *International risk and insurance.* First edition. London: McGraw-Hill.

Smit, M. 2009. Verbal communication with practitioner and risk expert. Pretoria. 22 September 2009.

Sobel, P. 2008. Risk management-based auditing. *Internal* Auditor, Vol. 65, No 4, pp. 92-93.

Software Engineering Institute (SEI). 2010. *Capability maturity model integration: overview.* [Online] Available from: http://www.sei.cmu.edu/cmmi/index.cfm. [Accessed: 4 March 2010].

Solomon, J. 2007. *Corporate governance and accountability*. Second edition. West Sussex: Wiley & Sons.

South Africa. National Treasury. 2010. *Departmental Financial Reporting Framework Guide - for the year ended 31 March 2010 (November 2009).* [Online] Available from: http://oag.treasury.gov.za [Accessed: 8 March 2010].

South Africa. National Treasury. 2009(a). *Public sector risk management framework.* [Online] Available from: http://oag.treasury.gov.za-/dev/content.asp?ContentId=592 [Accessed: 26 October 2009].

South Africa. National Treasury. 2009(b). *Internal audit framework*. Second edition. Office of the Auditor General. National Treasury. Pretoria. South Africa.

South Africa. 2008. Companies Act, No 71 of 2008. [Online] Available from: http://www.acts.co.za/companies-act-20089/index.htm [Accessed: 17 August 2009].

South Africa. 2008. Companies Bill, No 61B of 2008. Pretoria: State Printer.

South Africa. 2007. Corporate Laws Amendment Act, No 47 of 2007. Pretoria: State Printer.

South Africa. National Treasury. 2005. *Treasury regulations for departments, trading entities, constitutional institutions and public entities*. Issued in terms of the Public Finance Management Act, 1999. Pretoria: State Printer.

South Africa. 2004. Public Audit Act, No 25 of 2004. Pretoria: State Printer.

South Africa. 2003. Banks Amendment Act, No 19 of 2003. Pretoria: State Printer.

South Africa. 2003. Local Government: Municipal Finance Management Act (MFMA), No 56 of 2003. Pretoria: State Printer.

South Africa. Public Service and Administration. 2003. *The Batho Pele handbook on service delivery.* [Online] Available from: http://www.dpsa.gov.za/-documents.asp [Accessed: 20 March 2006].

South Africa. Public Service Commission. 2003. *Best practices on risk management frameworks for the public service.* [Online] Available from: http://www.psc.gov.za/docs/reports/soos/sick%20leave.pdf [Accessed: 6 December 2006].

South Africa. Public Service Commission. 2002. *Integrated risk management in the public sector: a provincial perspective*. [Online] Available from: http://www.psc.gov.za/docs/reports/soos/sick%20leave.pdf [Accessed: 6 December 2006].

South Africa. Department of Public Enterprises. 2002. *Protocol on corporate governance in the public sector*. Pretoria: State Printer.

South Africa. 1999. Public Finance Management Act (PFMA), No 1 of 1999 as amended by Act No 29 of 1999. Pretoria: State Printer.

South Africa. 1996. Constitution of the Republic of South Africa, No 108 of 1996, Twelfth Amendment Act of 2005. Pretoria: State Printer.

South African Government. Not dated. *South African government information*. [Online] Available from: http://www.info.gov.za/aboutgovt/dept.htm [Accessed: 13 March 2009].

South African Institute of Chartered Accountants (SAICA). 2010. *Companies Act & regulations latest information – 3 August 2010.* [Online] Available from: http://www.saica.co.xa/DesktopModules/EngagePublish/printerfriendly.aspx?itemID=1427 [Accessed: 31 August 2010].

South African Institute of Chartered Accountants (SAICA). 2009/10. *SAICA handbook: volume 2*. Lexis Nexis. South Africa.

South African Press Association (SAPA). 2007(a). *Leisurenet's duo day of reckoning comes*. 13 February 2007. [Online] Available from: http://www.money-web.co.za/mw/view/mw/page1743?oid+70165&sn+Detail [Accessed: 13 March 2009].

South African Press Association (SAPA). 2007(b). *Fidentia bosses in court.* 3 October 2007. [Online] Available from: http://www.fin24.com/articles/default/display_article.aspx?ArticleId=1518-24_214926 [Accessed: 13 March 2009].

Southern African Information Portal on Corruption. Not dated. *The South African strategic defence procurement package case study.* [Online] Available from: http://www.ipocafrica.org/cases/armsdeal/index.htm [Accessed: 13 March 2009].

Spencer Pickett, K.H. 2006*. Audit planning: a risk-based approach*. New Jersey: Wiley & Sons.

Spencer Pickett, K.H. 2005. *Auditing the risk management process*. New Jersey. Wiley & Sons.

Spencer Pickett, K.H. 2004(a). *The internal auditor at work: a practical guide to everyday challenges*. New Jersey. Wiley & Sons.

Spencer Pickett, K.H. 2004(b). How to spot and use the "new" internal auditors. *Journal of Corporate Accounting and Finance,* May/June 2004, pp. 29-36.

Spencer Pickett, K.H. 2003*. The internal auditing handbook*. Second edition. New Jersey. Wiley & Sons.

Spencer Pickett, K.H. 2000. Developing internal audit competencies. *Managerial Auditing Journal,* Vol. 15, No 6, pp. 265-278.

Spira, L.F. & Page, M. 2003. Risk management: the reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, Vol. 16, No 4, pp. 640-661.

Staciokas, R. & Rupsys, R. 2005. Internal audit and its role in organizational government. *Kaunas*, Issue 33, pp.169-181.

Steffee, S. 2009. In control. *Internal Auditor*, Vol. 66, No 6, pp. 47-49.

Sterck, M. & Bouckaert, G. 2006. International audit trends in the public sector. *Internal Auditor*, Vol. 63, No 4, pp. 49-53.

Storey, C.K. 2009. Breaking down silos. *Credit Union Management*, May, pp. 42-44.

Subramaniam, N., Ng, C. & Carey, P. 2004. Outsourcing internal audit services: an empirical study on Queensland public-sector entities. *Australian Accounting Review*, Vol. 14, No 3, pp. 86-95.

Sumners, G.E. 2008. *Study material for short course in risk.* Baton Rouge: Sumners Audit Services.

Sumners, G.E. & Soileau, J.S. 2008. Addressing internal audit staffing challenges. *EDPACS*, Vol. 37, No 3, pp. 1-11.

Sutton, S.G. & Hampton, C. 2003. Risk assessment in an extended enterprise environment: redefining the audit model. *International Journal of Accounting Information Systems*, Vol. 4, pp. 57-73.

Sverige, C. 2004. *The Parmalat scandal: Europe's ten-billion euro black hole.* [Online] Available from: http://www.wsws.org/articles/2004/jan2004/parm-j06.html [Accessed: 27 March 2009].

Swanson, G.A. & Marsh, H.L. 1991. *Internal auditing theory: a systems view*. New York: Greenwood Publishing.

Thiart, R. 2010. Telephonic conversation with the internal audit function of Old Mutual regarding the research interview. Pretoria. 4 March 2010.

Tricker, R.I. 2000. *Corporate governance: history of management thought series*. Aldershot, UK: Ashcroft Publishing.

Ttappous, M. 2009(a). (Maria@iiasa.org.za). 2009. Discussion of CIA statistics. [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 9 February 2009.

Ttappous, M. 2009(b). (Maria@iiasa.org.za). 2009. Discussion of entry requirements to sit for the CIA examination. [E-mail to:] Coetzee, G.P. (philna.coetzee@up.ac.za). 19 March 2009.

Turnbull Report. 1999. *Internal control: guidance for directors on the combined code.* [Online] Available from: http://www.frc.org.uk/corporate/reviews.cfm [Accessed: 12 February 2009].

Tustin, D.H., Ligthelm, A.A., Martins, J.H. & Van Wyk, H.deJ. 2005. *Marketing research in practice*. Pretoria: Unisa Press.

UK: *See* United Kingdom.

United Kingdom. Cabinet Office. 2002(a). *Risk: improving government's capability to handle risk and uncertainty - Full report.* Strategy Unit. London.

United Kingdom. Cabinet Office. 2002(b). *Risk: improving government's capability to handle risk and uncertainty - Annexes.* Strategy Unit. London.

United States of America. 2002. Sarbanes Oxley Act of 2002 (SOX). [Online] Available from: http://www.findlaw.com [Accessed: 6 December 2003].

United States of America. Agency for International Development. 1998. *Democracy and governance: a conceptual framework.* [Online] Available from:

http://www.usaid.gov/democracy/pdfs/pnacd395.pdf [Accessed: 6 December 2006].

USA: *See* United States of America.

Valsamakis, A.C., Vivian, R.W. & Du Toit, G.S. 2005. *Risk management: managing enterprise risk*. Third edition. Sandton: Heinemann Higher and Further Education.

Van der Nest, D.P. 2006. *Audit committees in the South African public service*. Unpublished DTech (Auditing) thesis. Tshwane University of Technology.

Van der Waldt, G. & Du Toit, D.F.P. 2005. *Managing for excellence in the public sector.* Second edition. Fourth impression. Landsdowne: Juta.

Van Gansberghe, C.N. 2005. Internal auditing in the public sector. *Internal Auditor,* Vol. 62, No 4, pp. 69-73.

Van Peursem, K. 2004. Internal auditors' role and authority: New Zealand evidence. *Managerial Auditing Journal*, Vol. 19, No 3, pp. 378-392.

Van Peursem, K. & Jiang, L. 2008. Internal audit outsourcing and rationales: SME evidence from New Zealand. *Asian Review of Accounting*, Vol. 16, No 3, pp. 219-245.

Van Wyk, A. 2009. *King III – apply or explain*. [Online] Available from: http://www.ciscorpgov.co.za/Anton%20van%20Wyk%20CIS%20Conference%20Presentation.ppt [Accessed: 7 October 2009].

Van Wyk, A. & Hodson, P. 1998. South Africa the rainbow nation. *Internal Auditor*, Vol. 55, No 2, pp. 20-22.

Van Zyl, A. 2010. *Jan en alleman besef nie hoe diep geldkrisis se gevolge lê.* Beeld, Sake 24, 16 July, pp. 1.

Vaughn, M. & Verstegen-Ryan, L. 2006. Corporate governance in South Africa: a bellwether for the continent? *Corporate Governance*, Vol. 14, No 5, pp. 504-512.

Vault. Not dated. *Internal consulting firms*. [Online] Available from: http://www.vault.com/articles/Internal-Consulting-Firms-15394310.html [Accessed: 8 May 2009].

Walayat, N. 2009. *Northern Rock: tax payer bailed out bankrupt ban adds to 750 million more losses.* [Online] Available from: http://www.marketoracle.co.uk/Article12516.html [Accessed: 26 August 2009].

Walker, P.L., Shenkir, W.G. & Burton, T.L. 2002. *Enterprise risk management: pulling it all together.* Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Wallace, W. 1984*. Time series analysis of the effect of internal audit activities on external audit fees.* Institute of Internal Auditors. Altamonte Springs. Florida.

Waring, C.G. 2006. Governance perspectives: there is more to be done. *Internal Auditor*, Vol. 63, No 6, pp. 35-37.

Watts, R.L. & Zimmerman, J.L. 1986. *Positive accounting theory*. New Jersey: Prentice-Hall.

West, A. 2009. The ethics of corporate governance: a South African perspective. *International Journal of Law and Management*, Vol. 51, no 1, pp. 10-16.

Wheeler, S. 2005. *A structured technique for applying risk based internal auditing in information technology environments*. Unpublished MCom (Computer Auditing) dissertation. University of Stellenbosch.

White, S.D. 2007. The auditors as internal consultant. *Internal Auditor*, Vol. 64, No 1, pp. 60-64.

Wikipedia. Not dated(a). *Empirical research.* [Online] Available from: http://en.wikipedia.org/wiki/Empirical research [Accessed: 4 June 2008].

Wikipedia. Not dated(b). *Risk*. [Online] Available from: http://en.wikipedia.org/wiki/Risk [Accessed: 4 June 2008].

Wikipedia. Not dated(c). *Accountability.* [Online] Available from: http://en.wikipedia.org?wiki?accountability [Accessed: 10 November 2006].

Wikipedia. Not dated(d). *Organisations.* [Online] Available from: http://en.wikipedia.org/wiki/Organisations [Accessed: 8 May 2009].

Wikipedia. Not dated(e). *Consultant.* [Online] Available from: http://en.wikipedia.org/wiki/Consultant [Accessed: 8 May 2009].

Wilkes, J. 2004. Corporate governance and measuring performance. *Measuring Business Excellence,* Vol. 8, No 4, pp. 13-16.

Williams, J.W. 2008. The lessons of Enron: media accounts, corporate crimes and financial markets. *Theoretical Criminology,* Vol. 471, No 12, pp. 471-499.

Wood, D. & Randall, S. 2004. Implementing ERM requires integrated approach. *Oil & Gas Journal*, Vol. 102, No 43, pp. 28-30.

Wynne, A. 2001. *Internal audit in Southern Africa.* [Online] Available from: http://accaglobal.com/trans-parency/publicsector/audit/internal.html [Accessed: 14 November 2005].

Yin, R.K. 2003. *Case study research: design and methods*. Third edition. Applied Social Research Methods Series, Vol. 5. London: Sage publications.

Zain, M.M. & Subramaniam, N. 2007. Internal auditor perceptions on audit committee interaction: a qualitative study in Malaysian public corporations. *Corporate Governance*, Vol. 15, No 5, pp. 894-908.

Ziegenfuss, D. 2010. A framework for audit evolution. *Internal Auditor*, Vol. 67, No 1, pp. 68-69.

Zikmund, W.G. 2000. *Business research methods*. Sixth edition. Harcourt: Harcourt College Publishers, Dryden Press.

ANNEXURE A

NATIONAL AND INTERNATIONAL THESES AND DISSERTATIONS RELATED TO THE STUDY (2000 to current)

Please note that the reference to a specific thesis or dissertation is copied directly from the document to ensure correctness according to the specific country's / institutions guidance.

An analysis of the development, status and functioning of audit committees at large listed companies in South Africa

B Marx, Doctor Commercii (Auditing), University of Johannesburg, 2008, Thesis

This study's research problem was to analyse the effective functioning of audit committees in the modern business environment, and the study aimed to investigate the factors and events that impact on the development, status and effective functioning of audit committees at large listed companies in South Africa. This was done through a comprehensive literature study of the factors impacting on audit committees and the empirical testing thereof at the largest listed companies in South Africa. The study found that audit committees are well established, properly constituted, have the authority and resources to effectively discharge their responsibilities and consist of members who act independently and who have the right mix of appropriate experience, financial literacy and financial expertise amongst their members. The audit committee's role was found to be generally well understood and supported by the board and the chief financial officers. It was further found that the audit committees are effective in discharging their oversight responsibilities on the board's behalf, with the only real exception being their effectiveness regarding IT-related aspects. However, audit committee reporting in annual reports was found to be of a poor standard and did not reflect the actual workings and effectiveness of the committee. It was also found that the audit committee's perceived responsibilities are evolving and that audit committee members' legal liabilities are increasing.

The development and evaluation of risk-based audit approaches
J Prinsloo, Masters in Accounting, University of the Free State, 2008, Dissertation

The purpose of the study is to trace the development of risk-based audit approaches, in order to understand the complexities and difficulties of these approaches, as well as to evaluate these risk-based audit approaches, with the objective of assisting in the process of improving the risk-based audit approach followed by the audit profession. Changing the risk-based audit approach is a normal consequence of the striving for the improvement and development of the services that the auditing profession provides. In developing the risk-based audit approach, there are certain complexities surrounding an audit that should be considered. The major complexities in the performance of an audit are: first, the expectation gap; second, the uncertainties surrounding the responsibilities of the auditor; third, the provision of reasonable assurance, and fourth, the practical implementation of audit standards. The auditing profession should, during this continuous process of changing the auditing standards and guidance, consider and evaluate changes against the theoretical foundations of auditing to support the credibility of the audit process. In conclusion, the author believes that the history of risk-based audit approaches has repeated itself and that the development of the risk-based audit approach and changes thereto were not considered against, and based on a sound foundation of auditing theory.

The role of internal auditing in corporate governance: qualitative and quantitative insights on the influence of organisational characteristics
G Sarens, Doctor, Ghent University, 2007, Dissertation

This study consists of six related papers, together aiming to provide a comprehensive picture of the internal audit profession. The six papers are, where applicable, referred to in this study's literature review. For consistency, the six papers and each paper's author(s) are listed below:

1	*The agency model as a predictor of the size of the internal audit function in Belgian companies*	G Sarens
2	*Building a research model for internal auditing: insights from literature and theory specification cases*	G Sarens & I De Beelde
3	*Internal auditor's perceptions about their role in risk management: a comparison between US and Belgian companies*	G Sarens & I De Beelde
4	*The relationship between internal audit and senior management: a qualitative analysis of expectations and perceptions*	G Sarens & I De Beelde
5	*A research note on the relationship between the control environment and the size of the internal audit function in Belgium*	G Sarens & I De Beelde
6	*The relationship between the control environment and the size of the internal audit function*	G Sarens

A structured technique for applying risk based internal auditing in information technology environments

S Wheeler, MAcc (Computer Auditing), University of Stellenbosch, 2006, Dissertation

The study aims to identify whether risk-based auditing methodology can be implemented in the IT environment. The IT infrastructure elements are linked to the business processes which they support. Their rankings are based on the risks assessments of the business process, the business process priority, the dependency of the business process on IT and the IT infrastructure element's own risk assessment. CobiT is used as an auditing method, i.e., best practice guidance to audit against.

The development of a risk management model supporting corporate governance in the City of Cape Town

P D Williams, MPA, University of Stellenbosch, 2004, Dissertation

The absence of a corporate mechanism or model for the City of Cape Town (City) makes it difficult to ensure that risks are addressed in an integrated manner. This research study seeks to provide an answer on how the City deals with risks relating to corporate governance in order to fulfil its constitutional and legislative obligations to its community in a sustainable manner. To develop a risk management model, models and approaches implemented at semi-private and private sectors organisations were analysed, and legislative requirements and specific developments on risk management in the public sector have been researched in an attempt to determine what local government is expected to do in addressing their risks The results revealed that:

- *The chief executive officers should reassess their organisation's corporate culture and set the 'tone from the top'. In the City's case the city manager has a critical role in balancing the need to address competitive forces and the need to consistently do the right things.*
- *Top management should constantly evaluate the completeness and appropriateness of corporate governance policies and practices as well as critical processes, internal controls and other risk management practices.*
- *The quality and competence of all staff need to be examined to determine if they understand government's challenges with regard to corporate governance.*
- *The development of a risk management model for the City will enable the organisation to pro-actively address its risks in this regard to fulfil its constitutional and applicable legislative requirements.*

An empirical investigation of turnover intentions of internal auditors
S V Williams, PhD, Virginia Commonwealth University, 2003

This study examines how outsourcing impacts turnover intentions of internal auditors. It proposes that outsourcing creates a degree of job insecurity and can result in undesirable changes in professional and organizational commitments and a higher probability of turnover intentions. I*nternal auditors respond to survey items that measure their psychological state (job insecurity), the consequences of job insecurity (professional commitment and organizational commitment), and the outcome (turnover intention). Structural equation modelling is used to analyze the relationships amongst the study variables. Results of the study show that internal auditors have relatively low levels of job insecurity and that there is a significant relationship amongst variables indicating that a high level of job insecurity negatively affects professional commitment and organizational commitment; and that this is positively related to turnover intention.*

The effect of inherent risk, knowledge spillover, and litigation risk on external auditors' reliance on client's internal audit functions
M Al-Harshani, PhD, University of Arkansas, 2003

The purpose of this study is to investigate the effect of inherent risk, knowledge spillover, and litigation risk on external auditors' reliance on audit clients' internal audit functions. An analytical model is developed to describe the theoretical relationship between external auditors' reliance and inherent risk as well as knowledge-spillover-related cost savings. External auditors engage in a cost-benefit analysis and select the optimal level of reliance on the internal audit function; that is when the marginal benefit and marginal cost of the reliance are equal. The empirical research findings indicate that external auditors' reliance on internal audit function is significantly and positively related to the audit client's financial condition. The results of this study fail to provide support for the existence of a relationship between the reliance on the internal audit function and inherent risk or knowledge spill-over. This implies that external auditors' reliance on the internal audit function is not significantly related to simultaneously

providing both audit and other services to the same audit client, an issue continuously being debated by accounting regulatory policy makers.

Risk and the South African private healthcare: an internal audit perspective
SP De la Rosa, Doctoral Thesis, University of Pretoria, 2003

This study aims at providing information on the major risks facing the private healthcare administration organisation in South Africa as well as the suitable corporate risk management methodology that may be applied in effectively managing these threats and opportunities from an internal audit perspective. The study includes empirical studies on:

- *the benefits of corporate risk management;*
- *concerns regarding corporate risk management;*
- *private healthcare;*
- *medical scheme risks;*
- *common language and strategies for risk management;*
- *uniform process and facilitation; and*
- *project management and continuous improvement.*

The results indicate that corporate risk management within the healthcare administration industry will become a cornerstone of effective business management; influencing the manner in which organisations of the future are structured and strategic planning is performed, improving corporate governance practices and allowing organisations to become pervasive in addressing new threats and possible areas of opportunities.

Internal corporate governance as a source of firm value: The impact of internal governance on the incidence of white collar crime
K A Schnatterly, PhD, University of Michigan, 2001

This study begins by investigating governance structures and their ability to impact the occurrence of white collar crime. It creates a framework relating

external and internal *governance to the occurrence of white collar crime, with firms that have announced a white collar crime from 1987-1998 forming the basis of the sample. Each of these firms is matched with a firm similar in size and scope, but from the year prior to the announcement, relating in 72 'crime firms' and 72 'non-crime firms'. The level of value loss is investigated. Discriminant analyses indicate that firms with crime and firms without crime have significantly different governance structures, and subsequent logit and regression tests indicate that firms with fewer crimes have stronger policies and procedures and stronger liaison roles. The firms with fewer crimes may also have more employee contingent pay, higher morale, boards paid with contingent compensation, fewer insiders on the audit committee, and less board ownership.*

Administrator's perceptions of internal auditing roles and effectiveness in Texas and Big Twelve public universities

C A Woodard III, EdD, Texas Southern University, 2000

This study examines presidents' and chief fiscal officers' perceptions of the importance of: (1) the role of internal auditing; and (2) selected factors utilized to evaluate auditing effectiveness. A non-experimental survey methodology was used to collect the data from public universities holding membership in the Texas Association of College and University Auditors and public universities who are members of the Big Twelve Athletic Conference. A survey scale was created consisting of three parts, namely:

- *activities undertaken by internal auditors in the performance of their work;*
- *criteria or factors utilized to evaluate auditing effectiveness; and*
- *items of a demographic nature.*

The results indicate significance differences in both presidents' and chief fiscal officers' perceptions of the importance of internal auditing's role. It further indicates significant differences in perceptions of presidents, chief fiscal officers and chief audit executives on the effectiveness of internal auditing. This study concludes that top administrators favour the traditional auditing roles of the

monitoring of compliance and internal controls. Additionally, chief audit executives can influence the perceived effectiveness of their departments by educating top administrators about the IIA and the IPPF.

The effect of internal audit outsourcing on financial statement users' confidence in their protection from fraudulent financial reporting
K L James, PhD, The University of Tennessee, 2000

The purpose of this study is to examine whether outsourcing the internal audit function enhances users' confidence in their protection from fraudulent financial reporting. Using source credibility theory, this study proposes that Big Five audit firms will be perceived as more competent and more objective than in-house internal audit departments and thus more likely to deter or detect and report fraudulent financial reporting. A between-subjects field experiment is performed in which the internal audit arrangement is the only independent variable. This arrangement is manipulated at four levels: (1) insourcing with the internal audit department reporting to senior management; (2) insourcing with the internal audit department reporting to the audit *committee; (3) outsourcing to the same Big Five firm that performs the external financial statement* audit *and (4) outsourcing to a Big Five firm different from the firm that performs the external financial statement audit. Dependent variables measure lenders' perceptions of the likelihood that fraud will be deterred, the likelihood that a committed fraud will be detected, and the likelihood that a detected fraud will be reported. Findings from this study suggest that to maximize user confidence in their financial reports, companies should either outsource their internal audit functions (whether to the same firm that performs the external audit or to another firm) or structure in-house internal audit departments to report to the audit committee.*

ANNEXURE B

Summary of Risk & Insurance Management Society (RIMS) risk maturity model steps

Initialisation	Risk specialisation	Enterprise wide risk awareness	Risk management integration	Enterprise risk management
STEP 1 **Ad-hoc**	**STEP 2** **Initial**	**STEP 3** **Repeatable**	**STEP 4** **Manageable**	**STEP 5** **ERM optimised**
▫ Limited executive support for risk management. ▫ Strategy is separate from risk management, need for integration is realised. ▫ Agreement on requirement for risk management policy and approach. ▫ Risk feedback takes place after losses. ▫ Limited implementation of standard assessments and criteria. ▫ Executives are aware of the need for increased skills to manage risks. ▫ Performance management does not look at benefits of risk, tangible or intangible.	▫ Executive awareness of need for formal risk management approach and process. ▫ Alignment between risk measures and strategic objectives. ▫ Agreement on requirement for risk management policy and approach. ▫ Agreement on roles, responsibilities and standardised risk assessment criteria. ▫ Guidance for developing of staff risk management capability. ▫ Evidence of improved performance outcome is limited.	▫ Senior management awareness of need for formal risk management approach and process. ▫ Goals and performance measures are linked. ▫ Proactive risk management policy is communicated. ▫ Risk management committee ensures compliances to framework. ▫ People encouraged and empowered to take well-managed risks. ▫ Evidence of improved performance is clear.	▫ Process owners incorporate risk management into their activities. ▫ Risk management is a formal part of goals and achievement. ▫ Reviews are conducted to actively manage risk management policy. ▫ Risk management policy is driven by business units heads via more quantitative measures. ▫ Staff has more risk management resources including training. ▫ Evidence of improved performance is significant.	▫ Business functions have embedded risk management. Performance improvement is risk driven. ▫ Risk management is integrated into strategy and planning. ▫ Risk management values are embedded into the strategic decision making process. ▫ Risk management committee ensures use of best practice and constant policy updates. ▫ Staff is empowered to manage risk and incorporate it into business activities. ▫ Evidence of improved performance is exceptional.

(Source: RIMS 2006)

ANNEXURE C

Maturity Model Criteria

Attributes	Define as	Non-existent	1 Ad-hoc	2 Initial	3 Repeatable	4 Managed	5 Optimised
Culture	Degree of executive support for a formalised risk management process.	No executive support for risk management is in place.	Organisational culture has little risk management accountability. Risk management is not interpreted consistently and focuses on post events.	Executives are aware of the need to manage uncertainty and risk and are committed to seeing a more formalised process being introduced.	Senior managers are aware of the need to manage uncertainty and risk and are committed to seeing a more formalised process being introduced.	Process owners incorporate the management of risks into all their activities.	The executives are regarded as exemplars of risk management with risk management embedded into each business function.
Involvement in strategy setting	The extent to which risk management is integrated with the organisation's strategy process.	The existing risk management approach (if any) is separate from strategy. The need for integration is not recognised.	The risk management process is separate from strategy. The need for integration is recognised.	Not all strategic objectives have risk measures and not all measures are linked with objectives.	The risk management process contributes to strategy and planning. All goals have measures and all performance measures are linked with goals.	The risk management process is an important part of strategy ad planning. Risks are aggressively considered as part of strategic planning. Risk manage-ment is a part of goal setting and achievement.	The risk management process is integrated into the strategy and planning process. The organisation measures the effectiveness of managing uncertainties and seizing risky opportunities.

Attributes	Define as	Non-existent	1 Ad-hoc	2 Initial	3 Repeatable	4 Managed	5 Optimised
Risk management policy setting	The risk policy articulates the executive's expectations of the risk management process.	No recognised need for a formalised risk management process.	A reactive risk management policy is in place to manage hazards only.	The need for proactive risk management approach and policy has been identified and accepted.	A proactive risk management policy has been drawn up and communicated.	Regular reviews are conducted to ensure that the values and goals included in the risk management policy are being lived and delivered upon.	Risk manage-ment values detailed in the policy are embedded into the strategic decision making process. Role model status is evident.
Risk management process	Articulation of the steps involved in conducting risk management at the strategic, tactical and process level.	No recognised need for a formalised risk management process.	There are no standardised risk assessment criteria. Standard collection and assessment processes are not identified. Risk feedback takes place only after a loss.	Agreement exists on a framework which describes roles and responsibilities. Standardised risk assessment criteria are also articulated. Mostly qualitative assessment methods are being used.	A risk management committee has been established to coordinate and review risk information and ensure compliance with the approved framework.	The processes articulated in the risk management framework are actively driven by the business unit heads. The increased use of quantitative risk measurement techniques is evident.	The risk management committee ensures the sharing of best practice initiatives across all business units and that the need for the framework to be updated is revisited at least annually.
People (staff)	People are equipped and supported to manage risk well.	Risk management skills are not considered important within the organisation.	Executives are aware of the need for increased skills to manage risks well.	Guidance is available within the organisation to develop the risk management capabilities of staff.	People are encouraged and supported to be innovative and are generally empowered to take well managed risks.	Staff has sufficient resources available to help them manage risks more effectively – this includes regular training.	Staff is empow-erred to be responsible for risk management and see it as inherent part of their business unit's activities. They have a good record of innovation and

Attributes	Define as	Non-existent	1 Ad-hoc	2 Initial	3 Repeatable	4 Managed	5 Optimised
							well managed risk taking.
Risk management performance	Risk management performance management is evident.	No recognised need to measure the effectiveness of the risk management programme.	Business case for introducing a more formalised risk management initiative does not include information on how the tangible and intangible benefits of risk management will be measured and reported back on.	Limited evidence of improved outcome performance consistent with improved risk management.	Evidence of significant improvements in outcome performance demonstrated by measures including stakeholder perceptions.	Clear evidence of significantly improved delivery of outcomes and showing positive and sustained improvement due to good risk management practices.	Excellent evidence of markedly improved delivery of outcomes against strategic objectives which compares favourable with other organisations employing risk management best practices.

(Source: RIMS 2006)

ANNEXURE D

Deliverables Matrix

Attributes	Defined as	1 Ad-hoc	2 Initial	3 Repeatable	4 Managed	5 Optimised
Culture	Degree of executive support for a formalised risk management process.	An overall vision and mission statement for the organisation has been set-up and communicated.	Values statement for the organisation has been set-up and communicated.	Values statement for the organisation includes 'positive risk taking' as a requirement for future success.	Self assessment of the organisation's culture takes place at least annually with results reviewed by the executive.	Results of ongoing self assessments of the organisation's culture are communicated to staff. Follow-up by management of unsatisfactory scores evident.
Involvement in strategy setting	The extent to which risk management is integrated with the organisation's strategy process.	Risk identification for strategic objectives takes place on an ad-hoc basis or usually performed to meet legislative requirements (e.g. annually for King 2 requirements, etc.).	• Risk identification forms part of the yearly strategic objective setting exercise of the organisation. • Significant risks are presented to the executive and other oversight committees on periodic reporting dates.	• Process in place to ensure that as strategic objectives are revised, that the formalised risk process is triggered. • Major risks for each of the strategic objectives are visible and monitored at monthly executive meetings.	• Major risks linked to strategic objectives have defined risk tolerance and appropriate risk indicators. • Feedback on progress in mitigating major risks forms part of the monthly management information pack.	• Risk dashboard reporting by strategic objective forms part of the monthly management information pack.

Attributes	Defined as	1 Ad-hoc	2 Initial	3 Repeatable	4 Managed	5 Optimised
Risk management policy setting	The risk policy articulates the executive's expectations of the risk management approach.	Ambit of risk management defined in SHE (health and safety) and other hazard guidelines.	Ambit of risk management articulated as part of the charter of an oversight committee, e.g. audit committee.	Ambit of risk management articulated in a distinct policy authored and owned by the CEO.	Self assessment of the organisation's compliance with the terms of the risk management policy is evident.	The organisation's culture assessment includes criteria to asses whether the principles and values of risk management detailed in its policy are being achieved.
Risk management process	Articulation of the steps involved in conducting risk management at the strategic, tactical and process level.	• Risk management process is articulated in SHE and other hazard guidelines. • Risk losses reported on a periodic basis.	• Simplified risk management process has been articulated into a paper presented to the executive and other oversight committees for information. • Executives issue notices on organisational risks which staff should be made aware of.	• Organisation wide risk management framework has been established. • The revision of the framework is coordinated through the risk management function located in the corporate business unit. • Annual audit of the risk management process is evident. • Common risk language initiated.	• Periodic input from the organisation on how the risk management framework should be adapted to meet their needs is evident. • Greater quantification of certain risk types is evident in the framework. • More consistent use of risk common language evident.	• Risk management components are integrated into the organisation's strategy and key policies. • Use of the framework's common risk language is evident throughout the organisation. • Benchmarking of the risk management process against international best practice is evident.
People (staff)	People are equipped and	• Risk management	• Need for internal risk champions	• Central risk manager role	Risk management training	• Tactical risk management

Attributes	Defined as	1 Ad-hoc	2 Initial	3 Repeatable	4 Managed	5 Optimised
	supported to manage risk well.	perceived to be predominantly a finance management function. • External training courses attended on a 'as needed' basis.	identified. • Risk management training for risk champions and managers outsourced to a third party.	identified and responsible person appointed. • Tactical risk management committee established to coordinate collation of risk information between internal risk champions and the designated risk manager.	programme brought in-house and made available to staff involved in the risk management process.	committee ensures staff is periodically trained on internal and external best practices. • Culture encourages employee participation in risk communication, such that it forms part of staff performance assessment.
Risk management performance	Risk management performance management is evident.	Performance measures focus on doing risk management to meet legislative requirements.	Performance measures focus on doing risk management to reduce the number of internal and external audit findings.	Performance measures focus on reducing the number of material surprises.	Performance measures focus on ensuring the strategic objectives of the organisation will be achieved within the boundaries of its approved risk appetite.	Performance measures involve indicators linked to risk appetite objectives and main competitors.

(Source: RIMS 2006)

ANNEXURE E

Risk Maturity Attributes and Levels (Key to table*)

Attributes	Maturity Levels					
	Level 5: Leadership	**Level 4: Managed**	**Level 3: Repeatable**	**Level 2: Initial**	**Level 1: Ad hoc**	**Non-existent**
1 Adoption of ERM- based approach	**Key Drivers: Degree of …** ▪ support from senior management, Chief Risk Officer ▪ business process definition determining risk ownership ▪ assimilation into support area and front-office activities ▪ far-sighted orientation toward risk management ▪ risk culture's accountability, communication and pervasiveness					
2 ERM process management	**Key Drivers: Degree of …** ▪ each ERM Process step (see definition) ▪ ERM Process's repeatability and scalability ▪ ERM Process oversight including roles and responsibilities ▪ risk management reporting ▪ qualitative and quantitative measurement					
3 Risk appetite management	**Key Drivers: Degree of …** ▪ risk-reward trade offs ▪ risk-reward-based resource allocation ▪ analysis as risk portfolio collections to balance risk positions					
4 Root cause discipline	**Key Drivers: Degree of …** ▪ classification to manage risk and performance indicators ▪ flexibility to collect and opportunity information ▪ understanding dependencies and consequences ▪ consideration of people, relationships, external, process and systems views					
5 Uncovering risks	**Key Drivers: Degree of …** ▪ risk ownership by business areas ▪ formalisation of risk indicators and measures ▪ reporting on follow-up activities ▪ transforming potentially adverse events into opportunities					
6 Performance management	**Key Drivers: Degree of …** ▪ ERM information integrated within planning ▪ communication of goals and measures ▪ examination of financial , customer, business process and learning ▪ ERM process goals and activities					
7 Business resiliency and sustainability	**Key Drivers: Degree of …** ▪ integration of ERM within operational planning ▪ understanding of consequences of action or inaction ▪ planning based on scenario analysis					

Key to table(*)

Level 1 – 5: Maturity levels

Attributes: Areas that must be addressed within the risk maturity scenario

Key drivers: Brief indication of the key drivers for the attribute, with a detailed explanation of each attribute within a specific maturity level explained below the table

Attribute 1: ERM-based approach

Degree of executive support for an ERM-based approach within the corporate culture. This goes beyond regulatory compliance across all processes, functions, business lines, roles and geographies. Degree of integration, communication and coordination of internal audit, information technology, compliance, control and risk management.

Non-existent
No recognised need for an ERM Process and no formal responsibility for ERM. Internal audit, risk management, compliance and financial activities might exist but are not integrated. Business process and risk ownership are not well defined.

Level 1: Ad hoc
Corporate culture has little risk management accountability. Risk management is not interpreted consistently. Policies and activities are improvised. Programs for compliance, internal audit, process improvement and IT operate independently and have no common framework, causing overlapping risk assessment activities and inconsistencies. Controls are based on departments and finances. Business processes and process owners are not well defined or communicated. Risk management focuses on past events. Qualitative risk assessments are unused or informal. Risk management is considered a quantitative analysis exercise.

Level 2: Initial
Risk culture is enforced by policy interpreted as compliance. An executive champions ERM management to develop an ERM Process. One area has used the ERM Process, as shown by the department head and team activities. Business processes are identified and ownership is defined. Risk management is used to consider risks in a far-sighted manner.

Level 3: Repeatable
ERM risk plans are understood by management and the organisation. Senior management expects that a risk management plan include a qualitative risk assessment for significant projects, new products, business practice changes, acquisitions, etc. Most areas use the ERM Process and report on risk issues. Process owners take responsibility for managing their risk and opportunities. Risk management creates and evaluates far-sighted scenarios.

Level 4: Managed
Risk culture is associated with career advancement. The organisation is self-governed with shared ethics and trust; promise-makers are held accountable. Risk management issues are understood at all levels and risk plans are conducted in all business process areas. The Board of Directors, CEO and CRO expect a risk management plan to include a qualitative risk assessment for significant projects, new products, business practice changes, acquisitions, etc. with reporting to the Board on priorities. All areas use the ERM Process to enhance their functions via the ERM framework, with frequent and effective communication on risk issues. Process owners incorporate managing their risks and opportunities within regular planning cycles. All areas create and evaluate far-sighted scenarios and follow-up activities.

Level 5: Leadership
Risk culture is analysed and reported as a systematic view of evaluating risk. Executive sponsorship is strong and the tone from the top has sewn an ERM Process into the corporate culture. Board of Directors, senior management and the CRO communicate risk management's importance in daily decisions. Risk management is embedded in each business function. Internal audit, information technology, compliance, control and

risk management are highly integrated and coordinate and report risk issues. All areas use risk-based best practices. The risk management lifecycle for each business process area is routinely improved.

Attribute 2: ERM process management

Degree of weaving the ERM Process into business processes and using ERM Process steps to identify, assess, evaluate, mitigate and monitor. Degree of incorporating qualitative methods supported by quantitative methods, analysis, tools and models. See ERM Process definitions.

Non-existent
There is little recognition of the ERM Process's importance.

Level 1: Ad hoc
Management is reactive and ERM might not yet be seen as a process. Few processes are standardised and are improvised instead. There are no standard risk assessment criteria. Risk management is involved in business initiatives only in later stages or centrally. Risk roles and responsibilities are informal. Risk assessment is improvised. Standard collection and assessment processes are not identified.

Level 2: Initial
Management recognises a need for an ERM Process. Agreement exists on a framework, which describes roles and responsibilities. Evaluation criteria are accepted. Risk mitigation activities are sometimes identified but not often executed. Qualitative assessment methods are used first in all areas and determine what needs deeper quantitative methods, analysis, tools and models.

Level 3: Repeatable
The ERM Process accommodates all business and support areas' needs. ERM is a process of steps to identify, assess, evaluate, mitigate and monitor. ERM Process includes the management of opportunities. An Enterprise Risk Council exists and senior management actively reviews risk plans. The ERM Process is collaborative and directs important issues to senior management.

Level 4: Managed
Management is clearly defined and enforced at every level. A risk policy articulates management's responsibility for risk management, according to established risk management processes. An Enterprise Risk Council exists and management develops and reviews risk plans. The ERM Process is coordinated with managers' active participation. Opportunities associated with risk are part of risk plans' expected outcome. Authentication, audit trail, integrity and accessibility promote roll-up information and information sharing. Periodic reports measure ERM progress for stakeholders, including the Board of Directors.

Level 5: Leadership
ERM, as a management aspect, is embedded in all business processes and strategies. Roles and responsibilities are process driven with teams collaborating across central and field positions. Risk and performance assumptions within qualitative assessments are routinely revisited and updated. The organisation uses an ERM process of sequential steps that improves decision-making and performance. A collaborative, enterprise-wide approach includes all supporters. Accountability for risk management is woven into all processes, support functions, business lines and geographies as a way to achieve goals.

Attribute 3: Risk appetite management

Degree of understanding the risk-reward trade-offs within the business. Accountability within leadership and policy to guide decision-making to attack gaps between perceived and actual risk. Risk appetite defines the boundary of acceptable risk and risk tolerance defines the variation of measuring risk appetite that management deems acceptable.

Non-existent
The need for formalising risk tolerance and appetite is not understood.

Level 1: Ad hoc
Risk management might lack a portfolio view of risk. Risk management might be viewed as risk avoidance and meeting compliance requirements or transferring risk through insurance. Risk management might be a quantitative approach focused on the analysis of high-volume and mission-critical areas.

Level 2: Initial
Risk assumptions are only implied within management decisions and are not understood outside senior leadership with direct responsibility. There is no ERM framework for resource allocation. Defining different views of business areas from a risk perspective cannot be easily created and compared.

Level 3: Repeatable
Risk assumptions within management decisions are clearly communicated. There is a structure for evaluating risk on an enterprise-wide basis and for gauging risk tolerance. Risks and opportunities are routinely identified, evaluated and executed in alignment with risk tolerances. The ERM framework quantifies gaps between actual and target tolerances as part of the ERM Process. Portfolio views to balance risk positions are created and risk tolerance is evaluated based on portfolio analysis.

Level 4: Managed
Risk appetite is considered in each ERM Process step. Resource allocation decisions consider the evaluation criteria of business areas. The organisation forecasts planned mitigation's potential effects versus risk tolerance as part of the ERM Process. Portfolio views are dynamic and risk tolerance is evaluated based on different views. Risk is managed by process owners. Risk tolerance is evaluated as a decision to increase performance and measure results. Risk-reward tradeoffs within the business are understood and guide actions.

Level 5: Leadership
A process for delegating authority to accept risk levels is communicated throughout the organisation. Risk management uncovers risk, reduces uncertainty and costs and increases return on equity by risk awareness. The management team and Enterprise Risk Council define tolerance levels for all departments. A mechanism compares and reports actual assessed risk versus risk tolerance. The organisation manages business areas and has portfolio collection to balance risk positions. Management prioritises resource allocation based on the gap between risk appetite and assessed risk and opportunity. The established risk appetite is examined periodically as part of planning. Example: Take more risk and gain more market share versus a conservative hold position and protect the brand.

Attribute 4: Root cause discipline

Degree of discipline applied to measuring problem's root cause and binding events with their process sources to drive the reduction of uncertainty, collection of information and measurement of the controls' effectiveness. The degree of risk from people, external environment, systems, processes and relationships is explored.

Non-existent
The effects of risky events might be identified but not linked to goals. Events are not associated with their process sources.

Level 1: Ad hoc
Cost savings are not evaluated based on risk-based consequences. Risks are not consistently evaluated. Perceived risk's frequency is not tracked or connected to a process. Risk indicators and goals are not organised within a framework and are not central to the ERM Process. Many root causes have a wide array of implications. Does not formally track root causes throughout the ERM Process.

Level 2: Initial
The cause and effect chain from the top-down and the bottom-up is not defined. Only past risk events are considered, leaving most possible risk areas not covered. A terminology and classification for collecting risk information exists. Awareness of a root cause approach's importance exists, but no robust scheme organises risk indicators or performance indicators as the core of a risk management framework and ERM Process.

Level 3: Repeatable
The cause and effect chain from the top-down and the bottom-up is understood. A terminology and classification for collecting risk information is used. The ERM framework is organised around root cause risk categories such as internal people, external environment, relationships, systems and processes. The root cause approach is important in each ERM Process step, from the Identify step, to ensure all risk sources' are reviewed, to the Monitor step, to verify that the problem – not the symptom – is attacked. Scenarios are developed and the root cause that makes the difference in scenario outcomes between worse case and best case are uncovered.

Level 4: Managed
A terminology and classification for collecting risk information is fully implemented. Causes, rather than only results, are identified, measured and managed. Risk and performance information is collected from all areas to identify dependencies and root cause indicators' frequency. Residual risk's financial implications are managed without distortive double counting within risk assessments. Operational, financial and strategic risks' root cause drivers are investigated, defined, quantified and routinely monitored. Scenario analysis is used throughout planning. Events are associated with their process sources to drive progress and measure the controls' effectiveness.

Level 5: Leadership
Mitigation measures are determined and a method to quantify effectiveness understood. There is an obvious focus on root cause to achieve goals and maximise risk's upside. The organisation uses "post mortems" to deconstruct past events (either its own or others') into root cause categories to prepare for future events. Scenarios are developed to evaluate potential benefits and drawbacks on a risk-adjusted basis. The organisation tracks events and traces root cause in evaluating cost benefits of improvements. Risk elements' frequencies are identified and monitored. The discipline of reviewing all risky avenues is promoted to provide a comprehensive view of risk and opportunity. This is proactive risk management, rather than problem management.

Attribute 5: Uncovering risks

Degree of quality and penetration coverage of risk assessment activities in documenting risks and opportunities. Degrees of collecting knowledge from employee expertise, databases and other electronic files (such as Microsoft® Word, Excel®, etc) to uncover dependencies and correlation across the enterprise.

Non-existent
There might be a belief that the most important risks are known, although there is probably little documentation.

Level 1: Ad hoc
Risk is owned by specialists, centrally or within a department. Risk information provided to risk managers is probably incomplete, dated or circumstantial, so there is high risk of misinformed decisions, with potentially severe consequences. Further mitigation, supposedly completed, is probably inadequate or invalid.

Level 2: Initial
Formal lists of risks for each department and discussions of risk are part of the ERM Process. Corporate risk indicators are collected centrally, based on past events. Departments might maintain their own informal risk checklists that affect their areas, leading to potential inconsistency, inapplicability, lack of sharing or under-reporting.

Level 3: Repeatable
An ERM team manages a growing list of business area specific risks, creating context for risk assessment as a foundation of the ERM Process. Risk indicator lists are collected by most process owners. Upside and downside outcomes of risk are understood and managed. Standardised evaluation criteria of impact, likelihood and controls' effectiveness are used, prioritising risk for follow-ups. Enterprise level information on risks and opportunities are shared. Risk mitigation is integrated with assessments to monitor effective use.

Level 4: Managed
Process owners aggressively manage a growing list of business area specific risk locally to create context for risk assessment activities as a foundation of the ERM Process. Risk indicators that are deemed critical to their areas are regularly reviewed in collaboration with the ERM team. Measures ensure downside and upside outcomes of risks and opportunities are aggressively managed. Standardised evaluation criteria of impact, likelihood and controls' effectiveness are used to prioritise risk for follow-up activity. Risk mitigation is integrated with assessments to monitor effective use.

Level 5: Leadership
Internal and external best practices, support functions, business lines and regions are systematically gathered and maintained. A routine, timely reporting structure directs risks and opportunities to senior management. The ERM Process promotes frontline employees' participation and documents risk issues' or opportunities' significance. Process owners regularly review and recommend risk indicators that best measure their areas' risks. The results of internal adverse event planning are considered a strategic opportunity.

Attribute 6: Performance Management

Degree of executing vision and strategy, working from the financial, customer, business process and learning and growth perspectives, such as Kaplan's balanced scorecard, or similar approach. Degree of exposure to uncertainty, or potential deviations from plans or expectations.

Non-existent
No formal framework of indicators and measure for goals and management exists.

Level 1: Ad hoc
Not all goals have measures and not all measures are linked with goals. Strategic goals are not articulated in terms that the frontline management understands. Compliance focuses on policy and is geared toward satisfying external oversight bodies. Process improvements are separate from compliance activities. Decisions to act on risks might not be systematically tracked and monitored. Monitoring is done and metrics are chosen individually. Monitoring is reactive.

Level 2: Initial
The ERM Process is separate from strategy and planning. A need for an effective process to collect information on opportunities and provide strategic direction is recognised. Motivation for management or support areas to adopt a risk-based approach is lacking.

Level 3: Repeatable
The ERM Process contributes to strategy and planning. All goals have measures and all performance measures are linked with goals. While compliance might trigger reviews, other factors are integrated, including process improvement and efficiency. The organisation indexes opportunities qualitatively and quantitatively, with consistent criteria. Risk management criteria are part of management's performance evaluations. Employees understand how a risk-based approach helps them achieve goals. Accountability toward goals and risk's implications are understood, and are articulated in ways that frontline personnel understand.

Level 4: Managed
The ERM Process is an integrated part of strategy and planning. Risks are aggressively considered as part of strategic planning. Risk management is a formal part of goal setting and achievement. Incentive for effective risk management is part of compensation and career development. Investment decisions for resource allocation examine the criteria for evaluating opportunity impact, timing and assurance. The organisation forecasts planned mitigation's potential effect on performance impact, timing and assurance prior to use. Employees at all levels use a risk-based approach to achieve goals.

Level 5: Leadership
The ERM Process is an important element in strategy and planning. Evaluation and measurement of performance improvement is part of the risk culture. Measures for risk management include process and efficiency improvement. The organisation measures the effectiveness of managing uncertainties and seizing risky opportunities. Deviations from plans or expectations are also measured against goals. A clear, concise and effective approach to monitor progress toward risk management goals is communicated regularly with business areas. Individual, management, departmental, divisional and corporate goals are linked with standard measurements.

Attribute 7: Business resiliency and sustainability

Extent to which the ERM Process's sustainability aspects are integrated into operational planning. This includes evaluating how planning supports resiliency and value. The degree of business ownership and planning beyond recovering technology platforms. Examples include vendor and distribution dependencies, supply chain disruptions, dramatic market pricing changes, cash flow volatility, business liquidity, etc.

Non-existent
Resiliency and sustainability is limited to an IT infrastructure orientation of continuity and disaster recovery.

Level 1: Ad hoc
Management is aware of resiliency-related risk and focused on infrastructure rather than the business. Users respond to disruptions with workarounds. The response to major disruptions is reactive. Departmental requirements to avoid risk often do not consider business needs. Impact of external and internal events on the business model is not systematically reviewed.

Level 2: Initial
The organisation recognises broader planning's importance. This highlights the business aspects in addition to traditional disaster recovery. There is recognition that resiliency is an issue that needs consideration in each ERM Process step, and not just in mitigation, as is common with traditional business impact analysis. Achieving balance between quarterly deliverables versus mid-term and long-term value is considered.

Level 3: Repeatable
Resiliency uses far-sighted scenario analysis to document key drivers. The organisation indexes priorities qualitatively and quantitatively, with consistent and objective criteria. Resiliency and sustainability are part of every risk plan and considered in each ERM Process step. Business model issues include geography, disruptive technology, competitors, leadership and environmental changes, with reporting and control by senior management.

Level 4: Managed
A comprehensive approach to resiliency considers the people, external, relationship, systems and process aspects. Logistics, security, resources and organisation of response procedures are well documented. Resiliency and sustainability are part of the ERM Process and business and business continuity as mitigation. As a result of the risk process's evaluation, business-driven impact analysis is initiated. Reporting on how external and internal events might impact the business model is raised to the Board of Directors. Balance is achieved between quarterly deliverables and mid-term and long-term value.

Level 5: Leadership
All issues are framed within the context of continuity of services to all stakeholders. Resiliency or sustainability might be defined differently by each organisation, with business-driven impact analysis initiated at all levels, based on priorities. Sustainability is not a reachable end state; rather, it is characteristic of a dynamic and evolving system. Long-term sustainability results from continuous adaptation.

(Source: RIMS 2006)

ANNEXURE F

Risk Maturity Model Score Card

(Adapted with the requirements in the second King Report) *

Organisation name: _____

Sector: _____

Information obtained: _____

Attributes	Step 1 Ad-hoc	Step 2 Initial	Step 3 Repeatable	Step 4 Managed	Step 5 Optimised	Step	Score
Culture (tone at the top)	Vision and mission statement.	Values statement.	Values statement includes 'positive risk taking'.	Annual self assessment of organisation's culture.	Ongoing self assessments of organisation's culture.		
Involvement in strategy setting	Annual risk identification for strategic objectives.	Risk identification part of strategic objective setting. Report significant risks to executive committee(s).	Risk process triggered when strategic objectives revised. Significant risks monitored at monthly executive meetings.	Board decides risk tolerance and indicators for major strategic objectives' risks. Monthly management feedback on progress in mitigating risks.	Risk on strategic objective part of monthly management information pack.		

Attributes	Step 1 Ad-hoc	Step 2 Initial	Step 3 Repeatable	Step 4 Managed	Step 5 Optimised	Step	Score
Risk management policy setting	Reactive policy to manage hazards only.	Need for proactive (hazards and opportunity) policy identified. Risk management in charter of over-sight committee (audit or risk).	Proactive policy. Risk management in policy 'owned' by CEO.	Regular self assessment of compliance with policy.	When assessing organisation culture (strategic decision making), measure achievement of principles and values in policy.		
Risk management process or framework	No formalised process. Risk losses reported on a periodic basis.	Simplified process for information purposes. Roles and responsibilities framework. Qualitative and standardised risk assessment. Executives issue notices on risks which staff should be made aware of.	Organisation-wide framework. Risk management committee. Risk management function revises the framework. Annual audit of the process. Common risk language initiated.	Periodic input from business unit heads on framework. Quantification of certain risk types. Consistent use of risk common language.	Framework components integrated into strategy and key policies. Framework's common risk language used across organisation. Benchmark against international best practice. Risk management committee: - ensures best practice across organisation; - review need to update framework annually.		
People (staff)	Risk management perceived as finance management function. External training courses on 'as needed' basis.	Need for internal risk champions identified. Training outsourced to third party. Guidance within organisation to develop capabilities.	Central risk manager (CRO) role identified and person appointed. Risk management committee coordinates internal risk champions and CRO.	Training programme in-house.	Risk management committee ensures staff periodically trained on internal and external best practices. Culture encourages employee participation in risk communication (forms part of performance assessment).		

Attributes	Step 1 Ad-hoc	Step 2 Initial	Step 3 Repeatable	Step 4 Managed	Step 5 Optimised	Step	Score
Risk management performance measures	Meet legislative requirements. No measure of benefits.	Reduce internal and external audit findings. Limited evidence of improved outcome.	Reduce number of material surprises. Measure improved outcome including stakeholders' perceptions.	Ensure strategic objectives will be achieved within boundaries of risk appetite. Clear evidence of improvement.	Indicators linked to risk appetite objectives and main competitors (best practice). Excellent evidence of improvement of strategic objectives.		
Internal audit (assurance provider) **	No formalised audit of risk management process.	Internal audit function performs overview of framework.	Internal audit function performs audit on certain areas of the framework.	*Ad hoc* audit of framework. Internal audit function provides input into framework.	Annual audit of framework. Internal audit function provides input into improving framework (ensure best practices).		
Reporting/ communica-tion ***	No communication regarding risk management.	Only internal communication to relevant parties.	Risk management included in financial statements as a sub-section.	Risk management included in financial statements as separate section.	Risk management included in financial statements as a separate section. Comprehensive reporting on all the elements of the framework. Separate risk management communication to external parties, e.g. risk report to shareholders.		
TOTAL							

(*) The empirical study was conducted early in 2009 and the third King Report (IOD 2009) was not yet available.
(**) As part of the criteria: sustainability (refer to section 3.6.2.2 on p. 211).
(***) Additional to the criteria as discussed in section 3.6.2.2 on p. 211 as a result of the guidance in the second King Report (IOD 2002).

ANNEXURE G

Private sector – top 40 companies listed on the JSE Limited as per market capital on 08/04/2009

Rank	Company	IIA member	Sector	Risk Maturity Attributes (*)								Total	Risk Maturity ≥120
				1	2	3	4	5	6	7	8		
1	BRITISH AMERICAN TOBACCO PLC	No	Tobacco retail	2	4	3	4	2	3	4	3	125	11
2	BHP BILLITON PLC	Yes	Mining	2	3	4	5	2	3	4	4	135	9
3	ANGLO AMERICAN PLC	Yes	Mining	2	4	3	4	2	3	3	3	120	12
4	SABMILLER PLC	Yes	Brewers	1	4	4	3	1	5	4	3	120	12
5	MTN GROUP LIMITED	Yes	Communication	1	5	4	5	3	4	3	5	150	6
6	SASOL LIMITED	Yes	Oil & Gas	1	3	2	3	2	3	4	3	105	Not mature
7	STANDARD BANK GROUP LIMITED	Yes	Banking	2	4	4	5	3	4	4	5	155	5
8	ANGLO PLATINUM LIMITED	Yes	Mining	1	4	3	2	2	4	4	5	125	11
9	ANGLOGOLD ASHANTI LIMITED	Yes	Mining	3	3	4	2	2	3	3	3	115	Not mature
10	IMPALA PLATINUM HOLDINGS LIMITED	Yes	Mining	3	4	5	5	2	5	5	5	170	2
11	COMPAGNIE FIN RICHEMONT	No	Consumer luxury goods	3	4	2	3	2	3	3	3	115	Not mature
12	FIRSTRAND LIMITED	Yes	Banking	2	3	4	4	4	4	5	3	145	7
13	GOLD FIELDS LIMITED	Yes	Mining	3	4	4	4	3	4	3	5	150	6
14	NASPERS LIMITED	No	Media	4	3	4	3	2	2	3	4	125	11
15	ABSA GROUP LIMITED	Yes	Banking	5	5	5	5	4	5	5	5	195	1
16	TELKOM SA LIMITED	Yes	Communication	3	4	5	5	4	4	5	4	170	2
17	KUMBA IRON ORE LIMITED	No	Mining	4	4	5	5	3	4	3	4	160	4
18	OLD MUTUAL PLC	Yes	Insurance	5	4	4	4	3	5	4	5	170	2
19	NEDBANK GROUP LIMITED	Yes	Banking	1	4	4	5	5	4	3	5	155	5
20	SANLAM LIMITED	Yes	Insurance	1	3	4	5	2	3	5	5	140	8
21	HARMONY GOLD MINING COMPANY LIMITED	Yes	Mining	1	5	4	4	3	4	4	4	145	7

Rank	Company	IIA Member	Sector	Risk Maturity Attributes (*)								Total	Risk Maturity ≥120
				1	2	3	4	5	6	7	8		
22	ARCELORMITTAL SA LIMITED	Yes	Iron & Steel	3	2	2	3	2	2	2	3	95	Not mature
23	REMGRO LIMITED	No	Investment	3	4	5	5	2	4	5	4	160	4
24	THE BIDVEST GROUP LIMITED	Yes	Business support	2	3	2	3	2	3	4	3	110	Not mature
25	LONMIN PLC	Yes	Mining	2	3	3	3	2	3	3	5	120	12
26	SHOPRITE HOLDINGS LIMITED	Yes	Retail	5	3	4	3	2	3	3	3	130	10
27	AFRICAN RAINBOW MINERALS LIMITED	Yes	Mining	1	2	2	2	1	2	2	3	75	Not mature
28	RMB HOLDINGS LIMITED	Yes	Banking	1	3	3	3	2	3	2	4	105	Not mature
29	EXXARO RESOURCES LIMITED	No	General mining	3	4	3	3	2	3	2	4	120	12
30	TIGER BRANDS LIMITED	Yes	Food products	1	3	3	3	2	4	3	3	110	Not mature
31	AFRICAN BANK INVESTMENTS LIMITED	Yes	Investment	3	4	3	4	2	3	4	4	135	9
32	LIBERTY INTERNATIONAL PLC	Yes	Investment	1	3	2	2	1	2	2	2	75	Not mature
33	PRETORIA PORTLAND CEMENT COMPANY LIMITED	Yes	Building materials	2	4	4	3	2	2	3	4	120	12
34	GROWTHPOINT PROPERTIES LIMITED	No	Real Estate	3	3	3	3	2	3	3	4	120	12
35	ASPEN PHARMACARE HOLDINGS LIMITED	Yes	Pharmaceuticals	1	4	4	3	2	3	4	3	120	12
36	REINET INVESTMENTS S.C.A (**)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
37	INVESTEC PLC	Yes	Banking	4	4	4	5	3	4	4	5	165	3
38	LIBERTY HOLDINGS LIMITED	Yes	Investment	1	3	3	3	2	2	3	3	100	Not mature
39	MASSMART HOLDINGS LIMITED	Yes	Retail	2	3	4	3	2	3	4	4	125	11
40	TRUWORTHS INTERNATIONAL LIMITED	Yes	Retail	1	3	3	3	2	4	5	3	120	12
41	DISCOVERY HOLDINGS LIMTED	Yes	Life insurance	1	3	3	3	3	4	4	5	130	10

(*) Score according to calculations as explained in section 5.2.1.3 on p. 303
(**) No information available as the company resides under Richmond (nr 11)

ANNEXURE H

Public sector – national government organisations as on 18/06/2009

NR	Department	IIA member	Risk Maturity Attributes (*)								Total	Risk Maturity ≥120
			1	2	3	4	5	6	7	8		
1	Department of Agriculture	Yes	3	2	2	2	1	1	1	3	75	Not mature
2	Department of Arts and Culture	Yes	2	3	3	2	1	2	4	3	100	Not mature
3	Department of Communication	Yes	1	1	2	1	1	1	2	1	50	Not mature
4	Department of Correctional Services	Yes	1	3	2	1	1	1	2	1	60	Not mature
5	Department of Defence	Yes	2	2	2	2	1	1	1	2	65	Not mature
6	Department of Education	Yes	2	2	1	1	1	1	1	1	50	Not mature
7	Department of Environmental Affairs and Tourism	Yes	2	1	1	1	1	1	1	1	45	Not mature
8	Department of Foreign Affairs	Yes	2	2	2	1	1	1	1	1	55	Not mature
9	Department of Governmental Communication	Yes	1	1	1	1	1	1	1	1	40	Not mature
10	Department of Health	Yes	1	2	2	2	1	1	2	1	60	Not mature
11	Department of Home Affairs	Yes	1	2	2	2	1	1	1	1	55	Not mature
12	Department of Housing	Yes	1	2	2	2	1	1	2	1	60	Not mature
13	Department of Independant Complaints Directorate	Yes	1	1	1	1	1	1	1	1	40	Not mature
14	Department of Justice and Constitutional Development	Yes	1	1	1	1	1	1	1	1	40	Not mature
15	Department of Labour	Yes	2	1	1	1	1	1	1	1	45	Not mature
16	Department of Land Affairs	Yes	1	1	1	1	1	1	1	1	40	Not mature
17	Department of Minerals and Energy	Yes	3	2	2	1	1	1	2	1	65	Not mature
18	National Intelligence Agency	Yes	1	1	1	1	1	1	1	1	40	Not mature
19	Department of National Treasury	Yes	1	1	1	1	1	1	1	1	40	Not mature
20	Department of Provincial and Local Government	Yes	2	2	2	1	1	1	2	2	65	Not mature
21	Department of Public Enterprises	Yes	1	2	2	3	2	2	3	3	90	Not mature
22	Department of Public Service and Administration	No	2	2	2	2	1	1	2	2	70	Not mature
23	Department of Public Service Commission	Yes	1	3	2	2	2	3	3	3	95	Not mature

NR	Department	IIA member	Risk Maturity Attributes (*)								Total	Risk Maturity ≥120
			1	2	3	4	5	6	7	8		
24	Department of Public Works	Yes	3	2	2	2	1	2	2	2	80	Not mature
25	Department of Science and Technology	Yes	2	2	2	2	2	3	4	3	100	Not mature
26	Department of Safety and Security	No	1	1	1	1	1	1	1	1	40	Not mature
27	Public Administration Leadership and Management Academy	No	3	2	2	3	2	3	3	3	105	Not mature
28	South African Police Service	Yes	1	2	2	2	1	2	2	2	70	Not mature
29	South African Revenue Service	Yes	2	3	4	3	2	3	3	3	115	Not mature
30	South African Secret Service (**)	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
31	Department of Social Development	Yes	3	2	2	2	1	3	3	3	95	Not mature
32	Department of Sport and Recreation	Yes	2	3	2	2	1	2	2	2	80	Not mature
33	Department of Statistics South Africa	Yes	1	1	1	1	1	1	1	2	45	Not mature
34	The Presidency	Yes	2	2	2	2	1	2	3	2	80	Not mature
35	Department of Trade and Industry	Yes	1	2	2	3	1	3	2	2	80	Not mature
36	Department of Transport	No	1	3	2	2	1	1	1	2	65	Not mature
37	Department of Water Affairs and Forestry	Yes	2	2	2	2	1	3	2	3	85	Not mature

(*) Score according to calculations as explained in section 5.2.1.3 on p. 303
(**) No information available

ANNEXURE I

Structured interview schedule

Private sector

1 Organisational background

1.1	Name of organisation:							
1.2	Sector:							
1.3	Name of interviewee(s):							
1.4	Position of interviewee(s):							
1.5	Indicate the estimated % of internal audit function (IAF) activities that are performed:							
	In-house consulting	Outsourced consulting	In-house assurance	Outsourced assurance				
1.6	Indicate the position of the IAF within the organisational structure:							
	Separate function	Part of financial department	Part of other department	Other				
1.7	Provide information on the staff component of the IAF:							
	Total number of full-time employees:							
	Total number of part-time employees:							
	Professional qualifications (number of full-time):	CA(SA)	CIA	CISA	Other			
	Tertiary academic qualifications (number of full-time):	Doctorate/ Master's	Honours/ B Tech degree	B degree/ Diploma	None			
	Internal audit experience (number of full-time):	>10 years	5–10 years	2–4 years	< 2 years			
	The use of consultants (in-house function only):	Always	When required	Seldom	Never			
	If 'always' or 'when required', indicate whether the IAF uses consultants to provide assurance and/or consulting activities with regard to the:							
	Risk management framework	Yes	No	Risk management process	Yes	No		
1.8	Provide information on the IAF's budget in terms of revenue and external audit fees:							
	Revenue:	Internal audit budget as % of revenue:	External audit fees:	Internal audit budget as % of external audit fees:				
1.9	Does the following exist within the organisational structure?							
	Audit committee	Risk committee	Risk department	Chief risk officer				

1.10	Indicate the composition of the audit committee:					
1.11	Indicate the composition of the risk committee:					
1.12	To which party does the chief audit executive (CAE) report functionally?					
	Audit committee	Chief executive officer	Chief financial officer	Other		
1.13	To which party does the CAE report administratively?					
	Audit committee	Chief executive officer	Chief financial officer	Other		
1.14	To which party/individual does the following report?					
	Risk department:					
	Chief risk officer:					
1.15	What is the extent of coordination between the following parties with regard to risk management?					
	• IAF and internal risk functions (risk department and/or chief risk officer):					
	Report relevant information to each other	Regular informative meetings	Copy each other on reports	Assist each other with duties	Other	
	If 'other', explain:					
	• Audit committee and risk committee:					
	Members serve on other committee	Read minutes of each other's meetings	Specific report to each other	Assist each other with duties	Not sure	Other
	If 'other', explain:					
	• IAF and risk committee:					
	IAF reports to risk committee regarding relevant findings on risk management	IAF provides risk committee with assurance regarding risk concepts	Risk committee asks IAF for input regarding risk concepts	IAF reports to risk committee regarding risk management responsibilities	Other	
	If 'other', explain:					
1.16	Do you agree with the risk maturity ranking of ……./200 (provide score sheet)?				Yes	No
	If 'no', explain:					

2 IIA *Standards*

(This section only focuses on the IIA *Standards* and excludes the rest of the International Professional Practices Framework.)

<table>
<tr><td>2.1</td><td colspan="6">Does the IAF adhere to the IIA Standards?</td></tr>
<tr><td></td><td colspan="2">Always</td><td colspan="2">Most of the time</td><td colspan="2">Never</td></tr>
<tr><td></td><td colspan="6">If ‘most of the time’, which broad area(s) are not covered?</td></tr>
<tr><td></td><td colspan="6">Provide reasons for why all areas are not covered:</td></tr>
<tr><td>2.2</td><td colspan="6">With regard to risk management, does your IAF adhere to IIA Standard 2120 (IIA 2009:28–29)? Do you think more guidance is needed from the IIA?</td></tr>
<tr><td></td><td>Activity</td><td colspan="3">Adherence</td><td colspan="2">More guidance</td></tr>
<tr><td></td><td>IAF evaluates the effectiveness of risk management (2120)</td><td>Yes</td><td>No</td><td>If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>IAF contributes to the improvement of risk management (2120)</td><td>Yes</td><td>No</td><td>If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>IAF evaluates the risk exposure of the organisation (2120.A1)</td><td>Yes</td><td>No</td><td>If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td>2.3</td><td colspan="6">With regard to the IAF’s annual plan, does your IAF adhere to IIA Standard 2010 (IIA 2009:25–26)? Do you think more guidance is needed form the IIA?</td></tr>
<tr><td></td><td>Activity</td><td colspan="3">Adherence</td><td colspan="2">More guidance</td></tr>
<tr><td></td><td>The IAF’s annual plan is risk-based, following the performance of an assessment (2010 & 2010.A1)</td><td>Yes</td><td>No</td><td>If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>The IAF accepts consulting engagements to improve risk management (2010.C1)</td><td>Yes</td><td>No</td><td>If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td>2.4</td><td colspan="6">With regard to performing a risk-based internal audit engagement, does your IAF adhere to IIA Standard 2201 and 2210 (IIA 2009:31–32)? Do you think more guidance is needed from the IIA?</td></tr>
<tr><td></td><td>Activity</td><td colspan="3" rowspan="2">Adherence</td><td colspan="2" rowspan="2">More guidance</td></tr>
<tr><td></td><td>For a specific audit engagement, the internal auditor:</td></tr>
<tr><td></td><td>considers the significant risks (2201)</td><td>Yes</td><td>No</td><td>If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>considers how risk is kept to acceptable levels (2201)</td><td>Yes</td><td>No</td><td>If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
</table>

	considers the adequacy of the relevant risk management process(es) (2201)	Yes	No	If 'no', provide reasons:	Yes	No
	considers the effectiveness of the relevant risk management process(es) (2201)	Yes	No	If 'no', provide reasons:	Yes	No
	performs a risk assessment to determine the engagement's objectives (2210.A1)	Yes	No	If 'no', provide reasons:	Yes	No

3 The changing internal audit environment

3.1	Do you think internal auditing should be involved in risk management with regard to:					
	providing assurance on the risk management framework	Yes	No	Provide reasons:		
	providing assurance on the risk management process	Yes	No	Provide reasons:		
	participating in consulting activities	Yes	No	Provide reasons:		
	taking full/partial responsibility for implementing the risk management framework	Yes	No	Provide reasons:		
	taking full/partial responsibility for implementing the risk management process	Yes	No	Provide reasons:		
3.2	Has the IAF's involvement in risk management increased over the past:					
	6 months	1 year	3 years	Since King II (2002)	Since King III (2009)	No
	If an increase has occurred, provide reasons:					
3.3	Do you anticipate that your IAF will, in the foreseeable future (the next 12 months), be increasingly involved in risk management owing to:					
	King III guidance	Current financial crisis	Board's changed needs	Management's changed needs	Other reasons	No
	If 'other reasons', explain:					

4 The risk management framework

(A risk management framework is the totality of the structures, processes, systems, methodology, individuals involved, etc. that an organisation uses to implement its risk management strategy – refer to Chapter 3, section 3.3.1.)

4.1	With regard to the organisation's risk management framework, which of the following activities are currently performed by the IAF, either as a consulting or as an assurance engagement? Simultaneously, indicate your perceptions on how these activities should be performed in future (refer to the IIA Position Paper: *Role of internal auditing in enterprise-wide risk management* (IIA 2004)).						
	Activity	Currently			In future		
		Consult	Assure	N/A	Consult	Assure	N/A
	Core internal audit roles						
	Providing assurance on the effectiveness of the risk management framework						
	Evaluating the methodology of the risk management process(es)						
	Evaluating the reporting of key risks						
	Reviewing the management of key risks						
	Legitimate internal audit roles with safeguards						
	Facilitating the identification and assessment of risks						
	Coaching management in responding to risks						
	Coordinating organisation-wide risk management activities						
	Developing the risk management framework						
	Maintaining the risk management framework						
	Roles internal auditing should not undertake						
	Setting the risk appetite						
	Taking part in the risk management process(es)						
	Taking decisions on risk responses						
	Implementing risk responses						
	Being accountable for risk management						
4.2	Indicate any further activities, not listed in question 4.1 above, that are currently performed/planned to be performed in future by your IAF:						
	Activity	Currently			In future		

		Consult	Assure	N/A	Consult	Assure	N/A

5 Risk management process

(The risk management process is used by management to identify, assess, treat, monitor and report on risks. It is usually a structured and systematic set of tasks, and the results of the process is a list of strategic/operational risks with relevant information on each risk, e.g. how the risk is treated – refer to Chapter 3, section 3.3.1.)

<table>
<tr><td>5.1</td><td colspan="9">Does your organisation have a risk management process for the following organisational levels:</td></tr>
<tr><td></td><td>Strategic</td><td>Yes</td><td>No</td><td>Operational</td><td>Yes</td><td>No</td><td>Organisation-wide integration</td><td>Yes</td><td>No</td></tr>
<tr><td>5.2</td><td colspan="9">If ‘yes’ at any of the levels in question 5.1, indicate the person(s) or department(s) responsible for executing the risk management process:</td></tr>
<tr><td></td><td>Strategic</td><td colspan="8"></td></tr>
<tr><td></td><td>Operational</td><td colspan="8"></td></tr>
<tr><td></td><td>Organisation-wide</td><td colspan="8"></td></tr>
<tr><td>5.3</td><td colspan="9">If ‘yes’ at any of the levels in question 5.1, indicate whether a risk register is kept:</td></tr>
<tr><td></td><td>Strategic</td><td>Yes</td><td>No</td><td>Operational</td><td>Yes</td><td>No</td><td>Organisation-wide integration</td><td>Yes</td><td>No</td></tr>
<tr><td>5.4</td><td colspan="9">If your organisation uses a risk register as indicated above, is the risk register:</td></tr>
<tr><td></td><td colspan="8">Electronically kept by using software</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td colspan="9">If ‘no’, how is the risk register kept?</td></tr>
<tr><td></td><td colspan="9">If ‘yes’, what software is used?</td></tr>
<tr><td></td><td colspan="9">How often is the risk register updated?</td></tr>
<tr><td></td><td>Continuously</td><td colspan="2">Monthly</td><td>Biannually</td><td colspan="2">Annually</td><td>Less frequently</td><td colspan="2">Not known</td></tr>
<tr><td></td><td colspan="6">Are the results of the internal audit engagements used to update the register (i.e. identification of additional risks during the audit)?</td><td>Yes</td><td>No</td><td>Not sure</td></tr>
<tr><td></td><td colspan="9">If ‘no’, provide reasons:</td></tr>
<tr><td>5.5</td><td colspan="9">Indicate the involvement of the IAF with regard to the risk management process(es):</td></tr>
<tr><td></td><td>No involve-ment</td><td>Audit the effectiveness of the process methodology</td><td>Audit the results of the process</td><td>Facilitates the process</td><td>Takes partial respon-sibility for the process</td><td>Takes full respon-sibility for the process</td><td>Other</td><td></td><td></td></tr>
</table>

	If 'other' involvement, indicate:

6 Annual planning of the IAF's activities

6.1	Does the IAF adhere to the following guidance (third King Report on Corporate Governance (IOD 2009:94)) for the planning of the function's activities?					
	Is the plan based on the performance of an assessment of risks and opportunities that may influence the strategic goals of the organisation?	Yes	Partially (%)	No		
	Are risks that were identified by management considered when drafting the plan?	Yes	Partially (%)	No		
	Are opportunities that were identified by management considered when drafting the plan?	Yes	Partially (%)	No		
	Is the plan aligned with the results of the risk management process(es)?	Yes	Partially (%)	No		
6.2	If answered 'partially' or 'no' to question 6.1, indicate when full adherence will be implemented:					
	Plan based on a risk and opportunities assessment performed	1 year	1–2 years	3–5 years	Never	N/A
	Plan based on risks identified by management	1 year	1–2 years	3–5 years	Never	N/A
	Plan based on opportunities identified by management	1 year	1–2 years	3–5 years	Never	N/A
	Plan aligned with the results of the risk management process(es)	1 year	1–2 years	3–5 years	Never	N/A
6.3	If answered 'partially' or 'no' to question 6.1, indicate your perceptions as to whether the following factors hinder the IAF in adhering to the guidance:					
	Lack of board commitment to risk management	No	Limited	Yes		
	Lack of board commitment to internal auditing	No	Limited	Yes		
	Lack of management commitment to risk management	No	Limited	Yes		
	Lack of management commitment to internal auditing	No	Limited	Yes		
	The IAF has limited resources	No	Limited	Yes		
	The IAF has limited available tools (e.g. IT software)	No	Limited	Yes		
	Other:	No	Limited	Yes		
	Other:	No	Limited	Yes		

7 Risk-based internal audit assurance engagements

7.1	When conducting the engagement planning, do you incorporate risk into the internal audit process by using the following (explain if needed):			
	COSO I model terminology	Yes	No	Not sure

	COSO II model terminology			Yes	No	Not sure
	If another methodology is used, indicate:					
7.2	If using the COSO II model, how is the following information obtained?					
	Information	Use auditee input	Use risk management process results (risk register)	No/limited information (internal auditor has to obtain)	Other (provide details)	
	Operational (auditee) objective setting					
	Risk identification for inherent risks					
	Risk assessment (measure) for inherent risks					
	Current risk mitigation activities					
	Risk assessment (measure) for residual risks					
7.3	When planning the internal audit engagement, which one or more of the following strategies are used as a starting point?					
	Previous year's working paper file	Inherent risks as per the risk register	Difference between the inherent and residual risk as per the risk register	Other		
7.4	When planning the internal audit engagement, which of the following are included?					
	Both threats and loss of opportunities are investigated as possible risks	The effect that a risk(s) may have on another area (outside the scope of the engagement) is considered	The effect that a risk(s) in another area (outside the scope of the engagement) may have on this engagement is considered	Recommending activities other than controls to mitigate risk to an acceptable level is considered		
7.5	Please describe any further aspect relevant to your organisation's internal audit engagement planning methodologies based on risk that was not covered in this questionnaire:					

8 Preliminary risk-based internal audit assurance engagement model

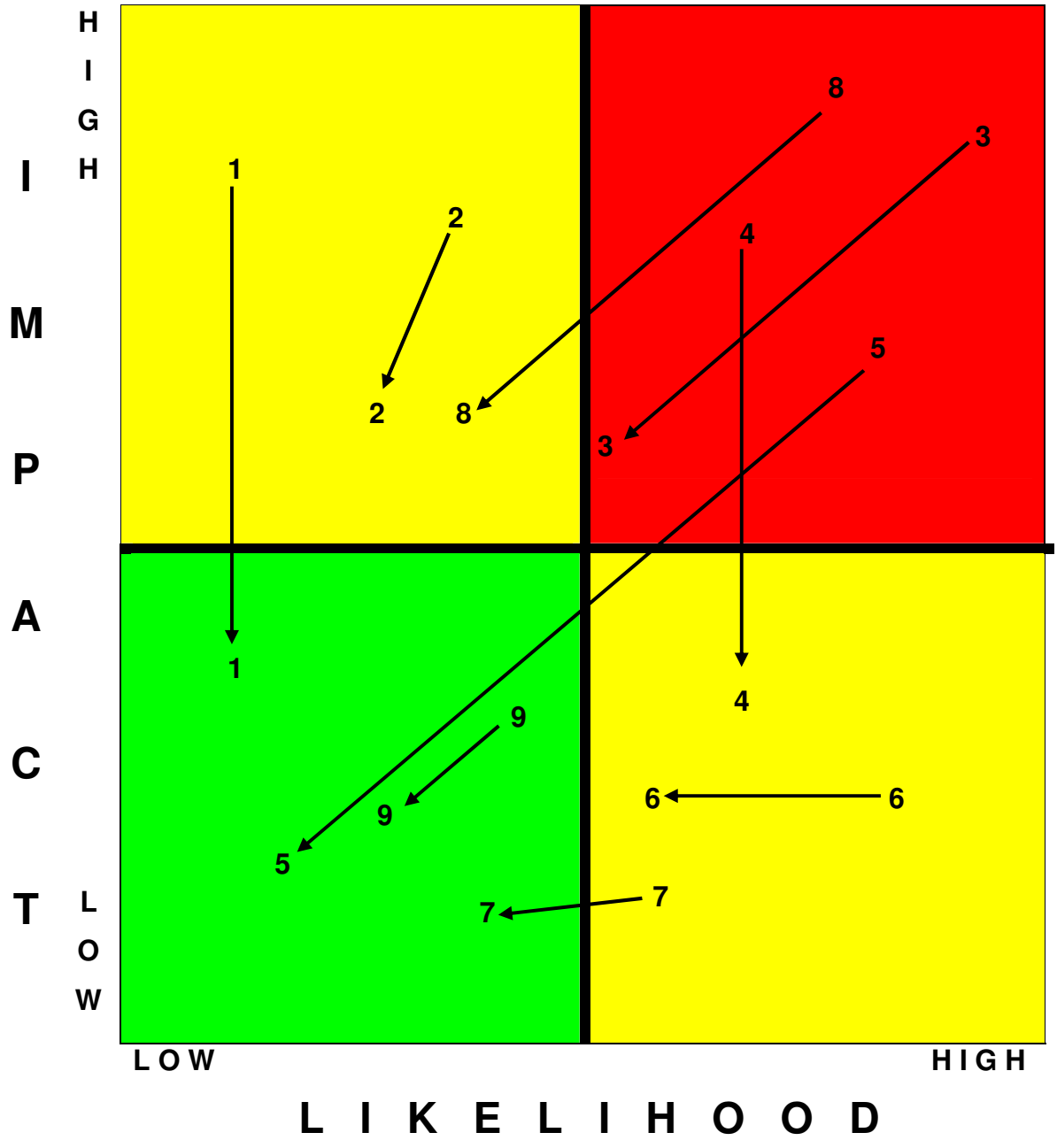
(Explain the model on p.11 to the interviewee(s).)

8.1	Do you think the model can be used when performing your internal audit assurance engagement?

	Yes	No	Reasons:
8.2	Do you think the model will reduce the extent of engagement procedures to be performed?		
	Yes	No	Reasons:
8.3	Do you think the model will be effective in focusing on the crucial aspects?		
	Yes	No	Reasons:
8.4	Do you think the model will be efficient (e.g. save time) whilst still being effective?		
	Yes	No	Reasons:

8.5	Do you think the model will assist in the following:			
	Eliminating ineffective controls	Yes	No	Reason:
	Eliminating unnecessary controls	Yes	No	Reason:
	Eliminating redundant controls	Yes	No	Reason:
	Eliminating excessive controls	Yes	No	Reason:
	Simplifying complex controls	Yes	No	Reason:

8.6	Do you think low inherent risks should be included in the audit planning (refer to no. 9 in model)?			
	Full inclusion	Only partial (judgment)	Only on surprise basis	No inclusion
	Provide reasons:			
8.7	Do you think a high inherent risk with a residual risk above the risk appetite should be included in the planning of audit procedures (refer to no. 2, 3, 4 & 8 in model)?			
	Must be included in full (audit all controls)	Only focus on adequacy of controls	Only focus on effectiveness of controls	Only an audit finding
	Provide reasons:			
8.8	Please provide any further comments that may be used to refine the model:			
8.9	May the model be tested at your organisation against a prior engagement?		Yes	No


HIGH
IMPACT
LOW
LOW
HIGH
LIKELIHOOD
1
2
8
3
4
5
9
6
7

ANNEXURE J

Structured interview schedule

Public sector

1 Organisational background

1.1	Name of organisation:						
1.2	Public sector cluster:						
1.3	Name of interviewee(s):						
1.4	Position of interviewee(s):						
1.5	Indicate the estimated % of internal audit function (IAF) activities that are performed:						
	In-house consulting	Outsourced consulting	In-house assurance	Outsourced assurance			
1.6	Indicate the position of the IAF within the organisational structure:						
	Separate function	Part of financial department	Part of other department	Other			
1.7	Provide information on the staff component of the IAF:						
	Total number of full-time employees:						
	Total number of part-time employees:						
	Professional qualifications (number of full-time):	CA(SA)	CIA	CISA	Other		
	Tertiary academic qualifications (number of full-time):	Doctorate/ Master's	Honours/ B Tech degree	B degree/ Diploma	None		
	Internal audit experience (number of full-time):	>10 years	5–10 years	2–4 years	< 2 years		
	The use of consultants (in-house function only):	Always	When required	Seldom	Never		
	If 'always' or 'when required', indicate whether the IAF uses consultants to provide assurance and/or consulting activities with regard to the:						
	Risk management framework	Yes	No	Risk management process	Yes	No	
1.8	Provide information on the IAF's budget in terms of expenditure and external audit fees:						
	Expenditure:	Internal audit budget as % of expenditure:	External audit fees:	Internal audit budget as % of external audit fees:			
1.9	Does the following exist within the organisational structure?						
	Audit committee	Risk committee	Risk department	Chief risk officer			

1.10	Indicate the composition of the audit committee:					
1.11	Indicate the composition of the risk committee:					
1.12	To which party does the chief audit executive (CAE) report functionally?					
	Audit committee	Chief executive officer	Chief financial officer	Other		
1.13	To which party does the CAE report administratively?					
	Audit committee	Chief executive officer	Chief financial officer	Other		
1.14	To which party/individual does the following report?					
	Risk department:					
	Chief risk officer:					
1.15	What is the extent of coordination between the following parties with regard to risk management?					
	• IAF and internal risk functions (risk department and/or chief risk officer):					
	Report relevant information to each other	Regular informative meetings	Copy each other on reports	Assist each other with duties	Other	
	If 'other', explain:					
	• Audit committee and risk committee:					
	Members serve on other committee	Read minutes of each other's meetings	Specific report to each other	Assist each other with duties	Not sure	Other
	If 'other', explain:					
	• IAF and risk committee:					
	IAF reports to risk committee regarding relevant findings on risk management	IAF provides risk committee with assurance regarding risk concepts	Risk committee asks IAF for input regarding risk concepts	IAF reports to risk committee regarding risk management responsibilities	Other	
	If 'other', explain:					
1.16	Do you agree with the risk maturity ranking of ……./200 (provide score sheet)?				Yes	No
	If 'no', explain:					

2 IIA *Standards*

(This section only focuses on the IIA *Standards* and excludes the rest of the International Professional Practices Framework.)

<table>
<tr><td>2.1</td><td colspan="8">Does the IAF adhere to the IIA Standards?</td></tr>
<tr><td></td><td colspan="3">Always</td><td colspan="3">Most of the time</td><td colspan="2">Never</td></tr>
<tr><td></td><td colspan="8">If ‘most of the time’, which broad area(s) are not covered?</td></tr>
<tr><td></td><td colspan="8">Provide reasons for why all areas are not covered:</td></tr>
<tr><td>2.2</td><td colspan="8">With regard to risk management, does your IAF adhere to IIA Standard 2120 (IIA 2009:28–29)? Do you think more guidance is needed from the IIA?</td></tr>
<tr><td></td><td colspan="3">Activity</td><td colspan="3">Adherence</td><td colspan="2">More guidance</td></tr>
<tr><td></td><td colspan="2">IAF evaluates the effectiveness of risk management (2120)</td><td>Yes</td><td>No</td><td colspan="2">If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td colspan="2">IAF contributes to the improvement of risk management (2120)</td><td>Yes</td><td>No</td><td colspan="2">If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td colspan="2">IAF evaluates the risk exposure of the organisation (2120.A1)</td><td>Yes</td><td>No</td><td colspan="2">If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td>2.3</td><td colspan="8">If answered ‘no’ to any of the above, indicate by when full adherence will be implemented:</td></tr>
<tr><td></td><td colspan="4">Evaluate effectiveness of risk management</td><td>1year</td><td>2–3years</td><td>3–5years</td><td>Never</td></tr>
<tr><td></td><td colspan="4">Contributes to improvement of risk management</td><td>1year</td><td>2–3years</td><td>3–5years</td><td>Never</td></tr>
<tr><td></td><td colspan="4">Evaluates the risk exposure of the organisation</td><td>1year</td><td>2–3years</td><td>3–5years</td><td>Never</td></tr>
<tr><td>2.4</td><td colspan="8">With regard to the IAF’s annual plan, does your IAF adhere to IIA Standard 2010 (IIA 2009:25–26)? Do you think more guidance is needed from the IIA?</td></tr>
<tr><td></td><td colspan="3">Activity</td><td colspan="3">Adherence</td><td colspan="2">More guidance</td></tr>
<tr><td></td><td colspan="2">The IAF’s annual plan is risk-based, following the performance of an assessment (2010 & 2010.A1)</td><td>Yes</td><td>No</td><td colspan="2">If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td colspan="2">The IAF accepts consulting engagements to improve risk management (2010.C1)</td><td>Yes</td><td>No</td><td colspan="2">If ‘no’, provide reasons:</td><td>Yes</td><td>No</td></tr>
<tr><td>2.5</td><td colspan="8">If answered ‘no’ to any of the above, indicate by when full adherence will be implemented:</td></tr>
<tr><td></td><td colspan="4">Risk-based plan based on risk assessment</td><td>1year</td><td>2–3years</td><td>3–5years</td><td>Never</td></tr>
<tr><td></td><td colspan="4">Accepts consulting engagements to improve the management of risks</td><td>1year</td><td>2–3years</td><td>3–5years</td><td>Never</td></tr>
</table>

2.6	With regard to **performing a risk-based internal audit engagement**, does your IAF adhere to IIA *Standard 2201* and *2210* (IIA 2009:31–32)? Do you think more guidance is needed form the IIA?					
	Activity	Adherence			More guidance	
	For a specific audit engagement, the internal auditor:					
	considers the significant risks (2201)	Yes	No	If 'no', provide reasons:	Yes	No
	considers how risk is kept to acceptable levels (2201)	Yes	No	If 'no', provide reasons:	Yes	No
	considers the adequacy of the relevant risk management process(es) (2201)	Yes	No	If 'no', provide reasons:	Yes	No
	considers the effectiveness of the relevant risk management process(es) (2201)	Yes	No	If 'no', provide reasons:	Yes	No
	performs a risk assessment to determine the engagement's objectives (2210.A1)	Yes	No	If 'no', provide reasons:	Yes	No

2.7	If answered 'no' to any of the above, indicate by when full adherence will be implemented:				
	Considering the significant risks	1year	2–3years	3–5years	Never
	Considering how risk is kept to acceptable levels	1year	2–3years	3–5years	Never
	Considering the adequacy of the relevant risk management process(es) performed	1year	2–3 ears	3–5years	Never
	Considering the effectiveness of the relevant risk management process(es) performed	1year	2–3years	3–5years	Never
	Performing a preliminary risk assessment to determine the engagement's objectives	1year	2–3years	3–5years	Never

3 The changing internal audit environment

3.1	Do you think internal auditing should be involved in risk management with regard to:			
	providing assurance on the risk management framework	Yes	No	Provide reasons:
	providing assurance on the risk management process	Yes	No	Provide reasons:
	participating in consulting activities	Yes	No	Provide reasons:
	taking full/partial responsibility for imple-menting the risk management framework	Yes	No	Provide reasons:

	taking full/partial responsibility for implementing the risk management process			Yes	No	Provide reasons:	
3.2	Has the IAF's involvement in risk management increased over the past:						
	6 months	1 year	3 years	Since PFMA (1999)	Since King II (2002)	Since King III (2009)	No
3.3	Do you anticipate that your IAF will, in the foreseeable future (the next 12 months), be increasingly involved in risk management owing to:						
	King III guidance	Current financial crisis	Executive's changed needs	Management's changed needs	Other reasons		No
	If 'other reasons', explain:						

3.4	If an increase has occurred, as stipulated in question 3.2, or will occur, as stipulated in question 3.3, indicate your perceptions as to whether the following events have and/or will have an effect on the involvement (either providing assurance, participating as consultants, or taking responsibility):			
	The growth in corporate governance guidance, specifically with regard to risk management	No effect	Moderate effect	Extreme effect
	The growth in corporate governance legislation, specifically with regard to risk management	No effect	Moderate effect	Extreme effect
	The complexity of the international environment (e.g. globalisation)	No effect	Moderate effect	Extreme effect
	The continual occurrence of financial scandals in the public sector	No effect	Moderate effect	Extreme effect
	The current global financial crisis, owing to the perception that risk management was not properly introduced	No effect	Moderate effect	Extreme effect
	The public's increased demand for accountability	No effect	Moderate effect	Extreme effect
	The IAF's status within the organisation	No effect	Moderate effect	Extreme effect
	The IAF's reputation within the organisation	No effect	Moderate effect	Extreme effect
	Internal auditing having an overall understanding of the organisation's environment	No effect	Moderate effect	Extreme effect
	Management perceive internal auditors to be control experts	No effect	Moderate effect	Extreme effect
	Management perceive internal auditors to be risk experts	No effect	Moderate effect	Extreme effect
	Other:	No effect	Moderate effect	Extreme effect
	Other:	No effect	Moderate effect	Extreme effect

4 The risk management framework

(A risk management framework is the totality of the structures, processes, systems, methodology, individuals involved, etc. that an organisation uses to implement its risk management strategy – refer to Chapter 3, section 3.3.1.)

4.1	With regard to the organisation's risk management framework, which of the following activities are currently performed by the IAF, either as a consulting or as an assurance engagement? Simultaneously, indicate your perceptions on how these activities should be performed in future (refer to the IIA Position Paper: *Role of internal auditing in enterprise-wide risk management* (IIA 2004)).						
	Activity	Currently			In future		
		Consult	Assure	N/A	Consult	Assure	N/A
	Core internal audit roles						
	Providing assurance on the effectiveness of the risk management framework						
	Evaluating the methodology of the risk management process(es)						
	Evaluating the reporting of key risks						
	Reviewing the management of key risks						
	Legitimate internal audit roles with safeguards						
	Facilitating the identification and assessment of risks						
	Coaching management in responding to risks						
	Coordinating organisation-wide risk management activities						
	Developing the risk management framework						
	Maintaining the risk management framework						
	Roles internal auditing should not undertake						
	Setting the risk appetite						
	Taking part in the risk management processes(es)						
	Taking decisions on risk responses						
	Implementing risk responses						
	Being accountable for risk management						
4.2	Indicate any further activities, not listed in question 4.1, that are currently performed/planned to be performed in future by your IAF:						
	Activity	Currently			In future		

		Consult	Assure	N/A	Consult	Assure	N/A

4.3	Indicate your perceptions as to whether the following factors hinder the IAF in providing a service with regard to the risk management framework within your organisation:			
	IAF's lack of knowledge of the organisation	No	Limited	Yes
	Internal auditor's lack of general risk knowledge	No	Limited	Yes
	Limited skills of the internal audit staff complement	No	Limited	Yes
	Limited competencies of the audit staff complement	No	Limited	Yes
	Limited available tools (e.g. IT software) to assist internal auditing	No	Limited	Yes
	Limited resources available to the IAF	No	Limited	Yes
	Expectations of management of duties to be performed by IAF too broad	No	Limited	Yes
	Internal auditing has no/limited access to senior management	No	Limited	Yes
	Internal auditing has no/limited access to the audit committee	No	Limited	Yes
	Internal auditing has no/limited access to the risk department	No	Limited	Yes
	Internal auditing has no/limited access to the chief risk officer	No	Limited	Yes
	Internal auditing has no/limited access to the risk committee	No	Limited	Yes
	The overall risk management strategy is ineffective	No	Limited	Yes
	The organisation has a low risk maturity	No	Limited	Yes
	Other:	No	Limited	Yes
	Other:	No	Limited	Yes
4.4	Provide any additional information on possible problem areas regarding question 4.3:			

5 Risk management process

(The risk management process is used by management to identify, assess, treat, monitor and report on risks. It is usually a structured and systematic set of tasks, and the results of the process is a list of strategic/operational risks with relevant information on each risk, e.g. how the risk is treated – refer to Chapter 3, section 3.3.1.)

5.1	Does your organisation have a risk management process for the following organisational levels:								
	Strategic	Yes	No	Operational	Yes	No	Organisation-wide integration	Yes	No

5.2	If 'yes' at any of the levels in question 5.1, indicate the person(s) or department(s) responsible for executing the risk management process:	
	Strategic	
	Operational	

	Organisation-wide								
5.3	If 'yes' at any of the levels in question 5.1, indicate whether a risk register is kept:								
	Strategic	Yes	No	Operational	Yes	No	Organisation-wide integration	Yes	No
5.4	If your organisation uses a risk register as indicated above, is the risk register:								
	Electronically kept by using software							Yes	No
	If 'no', how is the risk register kept?								
	If 'yes', what software is used?								
	How often is the risk register updated?								
	Continuously	Monthly	Biannually	Annually	Less frequently	Not known			
	Are the results of the internal audit engagements used to update the register (i.e. identification of additional risks during the audit)?						Yes	No	Not sure
	If 'no', provide reasons:								
5.5	Indicate the involvement of the IAF with regard to the risk management process(es):								
	No involve-ment	Audit the effectiveness of the process methodology	Audit the results of the process	Facilitates the process	Takes partial respon-sibility for the process	Takes full responsi-bility for the process	Other		
	If 'other' involvement, indicate:								

6 Annual planning of the IAF's activities

6.1	Does the IAF adhere to the following legislation (*PFMA No 1 of 1999* (Section 38) and Treasury Regulations (par 3.2.1 and 3.2.7)) and guidance (third King Report on Corporate Governance (IOD 2009:94)) for the planning of the function's activities?			
	Is the plan based on the assessment of key risk areas?	Yes	Partially (%)	No
	Are risks that were identified by management considered when drafting the plan?	Yes	Partially (%)	No
	Are opportunities that were identified by management considered when drafting the plan?	Yes	Partially (%)	No
	Are the current operations taken into account?	Yes	Partially (%)	No
	Are the proposed operations in the organisation's strategic plan taken into account?	Yes	Partially (%)	No
	Is the organisation's risk management strategy taken into account?	Yes	Partially (%)	No
	Is the plan aligned with results of the risk management process(es)?	Yes	Partially (%)	No
6.2	If answered 'partially' or 'no' to question 6.1, indicate when full adherence will be implemented:			

	Plan based on the assessment of key risk areas	1year	2–3years	3–5years	Never
	Plan based on risks identified by management	1year	2–3years	3–5years	Never
	Plan based on opportunities identified by management	1year	2–3years	3–5years	Never
	Current operations taken into account	1year	2–3years	3–5years	Never
	Proposed operations in the organisation's strategic plan taken into account	1year	2–3years	3–5years	Never
	Risk management strategy of the organisation taken into account	1year	2–3years	3–5years	Never
	Plan aligned with results of the risk management process(es)	1year	2–3years	3–5years	Never
6.3	If answered 'partially' or 'no' to question 6.1, indicate your perceptions as to whether the following factors hinder the IAF in adhering to the guidance:				
	Lack of management commitment to risk management	No	Limited	Yes	
	Lack of management commitment to internal auditing	No	Limited	Yes	
	Lack of executive commitment to risk management	No	Limited	Yes	
	Lack of executive commitment to internal auditing	No	Limited	Yes	
	The IAF has limited resources	No	Limited	Yes	
	The IAF has limited available tools (e.g. IT software)	No	Limited	Yes	
	The overall risk management strategy is ineffective	No	Limited	Yes	
	The organisation has a low risk maturity	No	Limited	Yes	
	Other:	No	Limited	Yes	