The use of risk management principles in planning an internal audit engagement

P. Coetzee & D. Lubbe

ABSTRACT

With the current growth in awareness of the value of internal audit services, the increased demand from various stakeholders, and the scarcity of competent internal auditors, the profession needs a new mindset, particularly in respect of the execution of internal audit activities. Although risk-based internal auditing is a fairly new concept, its implementation could assist internal auditors to audit 'smarter', that is, more effectively and efficiently. However, it is unclear whether the current concept of a risk-based internal audit engagement is in line with modern business practices, such as enterprise-wide risk management principles. Furthermore, it is also uncertain whether internal auditors share a single set of risk management principles and concepts, and how (or even if) these should be included in the internal audit engagement. This article explores the common understanding of what the planning phase of a risk-based internal audit engagement should entail when based on risk management principles, and identifies the organisational elements that should be in place that would make it easier for internal auditors to implement such a risk-driven approach when conducting engagements. The research methodology involved a literature review and structured interviews with chief audit executives of risk-mature organisations. The findings support the existence of uncertainty among chief audit executives regarding the use of risk management principles when performing risk-based internal audit engagements. Chief audit executives also appeared uncertain how to apply these principles to the planning and execution of internal audit

Prof. P. Coetzee is an associate professor in the Department of Auditing, University of Pretoria. Prof. D. Lubbe is in the Centre for Accounting, University of the Free State. E-mail: philna.coetzee@up.ac.za

engagements. Gaps and shortcomings identified by the research should be addressed by the Institute of Internal Auditors through developing more comprehensive guidance for their members.

Key words: risk management, key risks, internal auditing, risk-based internal auditing, internal audit engagement

Introduction

Internal auditing and the profession's role within the organisation constitute a dynamic and ever-changing environment. PricewaterhouseCoopers (PwC 2008b: 2), after conducting a study to determine the perceived future status of internal auditing, concluded that, due to the rapid growth of the profession and the many changes in the business environment, if internal audit wanted to remain a role-player in the future, it was essential for the profession to adopt a new mindset. This is supported by the 2012 PricewaterhouseCoopers studies in which, firstly, chief executive officers (PwC 2012: 3) identified the emerging risk areas as growth, particularly as growth is increasingly associated with innovation, and the new skills that are needed in order to participate in this growth. Secondly, heads of internal audit functions indicated (PwC 2012: 5–6) that they were responding to this challenge by being willing to play a significant role in a changed business environment. This latter statement is further substantiated by the many recent changes made by the Institute of Internal Auditors (IIA) to their issued guidelines, and in the research performed to gain insight into the changing role of internal auditing (IIARF 2007: 344–351; E&Y 2008: 2; PwC 2008b: 31–39; IIARF 2009: 1; IIARF 2011: V).

One of these fundamental changes in the profession is the incorporation of risk management principles into the internal audit function's activities. This can be attributed to the increased interest in and implementation of risk management in the broader business environment (IIARF 2009: 9; Castanheira, Rodrigues & Craig 2010: 89–94). Sound governance principles require internal auditors to assist management in mitigating the key risks (IOD 2009: 94–95). Therefore, when internal audit activities such as internal audit engagements are performed, the focus of the audit procedures should be on the key risks threatening the operational objectives of the business unit or the business process under review, and on performing a reduced number of audit procedures, or even none at all, on the low-risk areas. This is also referred to as risk-based internal auditing.

The literature is replete with studies and discussions that refer to risk-based internal auditing (McNamee & Selim 1998: 199; Spencer Pickett 2003: 12; Griffiths

2006b: 43; IOD 2009: 94; Soh & Martinov-Bennie 2011: 612. Most reflect on the role that internal auditing should play with regard to the overall risk management strategy of the organisations that is developed and implemented by management (also referred to as 'enterprise risk management'). Other literature (Pelletier 2008: 73; Koutoupis & Tsamis 2009: 106; IOD 2009: 94; Hamid 2012: 343) refer to the internal audit function's annual plan, based on the organisation's strategic risks, when using the term 'risk-based internal auditing' (also referred to as 'macro risk-based internal auditing'). However, as these contrasting examples of the use of the term 'risk management' illustrate, as a relatively new concept within the internal audit environment, the incorporation of risk within the internal audit function's activities is sometimes misunderstood. A study of Greek banks' internal audit methodologies by Koutoupis & Tsamis (2009: 102) revealed that many internal audit functions, although declaring that they are using a risk-based approach in their activities, could not prove it, thus adding further to the confusion in the use of the term 'risk-based internal auditing'.

The concept of risk-based internal auditing using risk management principles for the performance of operational internal audit engagements, performed on either a business unit or on a business process (also referred to as 'micro risk-based internal auditing'), is even less well explored. Very few published articles explore this concept, and it seems that this paucity of studies mirrors the low implementation of this style of audit. For example, the results of a study performed by Castanheira et al. (2010: 95) revealed that while most respondents indicated that they did perform risk-based planning when preparing their annual internal audit plan, only one third made use of risk management principles in their engagement planning.

Apart from these challenges to comprehensively identifying the concept of risk-based internal auditing, and the difficulties experienced in attempting to apply theory to practice, the internal audit profession now needs to perform their activities even more effectively and efficiently due to a worldwide shortage of competent internal auditors. In South Africa, the Sector Education and Training Authority (SETA) for the Finance, Accounting, Management Consulting and Other Financial Services sector (FASSET 2011) recognises internal auditing as a scarce skill for the sector. A possible way of balancing the limited number of skilled internal auditors available against the growing needs of the organisation is for internal auditors to change from a control-driven approach to a business risk-driven approach (IOD 2009: 96), thus focusing more on the key risk areas of the organisation, instead of trying to include controls in their assurance activities. While this could mean that fewer audit procedures are performed, it does ensure that all key risks areas are more effectively

covered during the internal audit engagement, resulting in the efficient use of internal auditors and audit resources.

There is thus a clear need to establish whether risk management principles can be incorporated into the concept of a risk-based internal audit engagement, and if so, whether it is being done in practice. This research will also broaden the knowledge of risk-based internal audit engagements, as published information seems to be limited. The results will provide the profession with insight into whether its guidance is relevant and being adhered to in practice. The research results, and the IIA's response through its guidelines, should assist practitioners in understanding what risk-based internal auditing entails, and which organisational elements should incorporate risk methodology into the policies and procedures of their internal audit functions.

To address this need, the research objectives of this study were two-fold: firstly, to determine what organisational elements have to be in place in order to perform a risk-based internal audit engagement based on risk management principles; and secondly, to determine how the risk management principles can be incorporated into the planning phase of a risk-based internal audit engagement. For both these research objectives, a literature study was conducted, whereupon the theory was formulated and tested in an empirical study.

Research methodology

To achieve the research objectives, the researcher targeted two areas for research. Firstly, a literature review was conducted, with the intention of identifying the organisational elements that should be in place for internal auditing to be able to perform a risk-based internal audit engagement based on risk management principles. The literature review was then expanded in order to understand how the risk management principles could be incorporated into the planning phase of an internal audit engagement. Although an internal audit engagement consists of four phases (as discussed in the literature review), this article focuses only on the first phase (planning), as this sets the parameters that guide the performance of the rest of the audit engagement.

Secondly, the views of the heads of prominent internal audit functions within the private and the public sectors (hereafter referred to as 'chief audit executives') were obtained on whether the organisational elements that are needed to perform risk-based internal auditing exist within their organisations, and whether risk management principles are being applied in the planning phase of an internal audit engagement.

Formal interviews were conducted with five chief audit executives from each of the private and the public sectors (refer to Annexure A). It was decided to choose five organisations in each sector as a starting point, and if the data were not saturated, further interviews were to be conducted. The organisations were chosen on the basis of their level of risk maturity (i.e. the extent to which the elements within the organisation's risk management strategy have been adopted and implemented), as well as the risk maturity of their internal audit functions. The reasoning behind this decision was that risk management, as part of the governance structure of an organisation, is a relatively new concept, and if a specific organisation and its internal audit function was risk mature, there was a higher probability that internal auditors would follow a risk-based approach when performing internal audit engagements. The methodology followed is discussed in the subsection on risk maturity.

Although a structured questionnaire was developed for each sector, to guide the interviewer, face-to-face interviews were conducted with each of the ten chief audit executives. This decision was motivated by the fact that the risk-based internal audit engagement is a fairly new concept (refer to the discussion in the literature review) and although organisations may believe that they are following a risk-driven approach, it is possible that their internal audit engagements still focus on compliance with controls, albeit with a stronger focus on risk (control-driven approach); and furthermore, it was anticipated that the respondents' participation would be more committed when given the opportunity to discuss and debate the issues being raised by the interviewer.

A limitation of the study was that only ten South African organisations were surveyed. However, this was offset by the following positive aspects: each interview was conducted using a structured questionnaire as its basis; respondents were provided with an explanation of the terminology, and of their organisation's risk maturity score; the responding organisations were chosen based on their high risk-maturity levels; interviews were conducted with the chief audit executives of risk-mature internal audit functions, and the data gathered were saturated. All of these factors enhanced the quality of the data. Another limitation was that the study only focused on the initial planning phase of an internal audit engagement. Although the IIA's mandatory guidance on an internal audit engagement identifies four phases (IIA 2011: 16–23), this article focuses only on the initial planning phase essentially because it sets the tone for the rest of the activities to be performed during the audit engagement.

Organisational elements enabling a risk-based approach

In this section, the literature supporting the first research objective is discussed, namely the elements that should be in place before a risk-based internal audit engagement can be performed.

The IIA (2011: i) describes the internal audit engagement as requiring a systematic and disciplined approach. This statement is supported by Lemon and Tatum (2003: 270), who observe that this approach is similar to the systematic manner in which an external audit is performed, as required by the International Standards on Auditing (SAICA 2009/10: ISA200-2). Thus, performing an internal audit engagement requires a structured approach, regardless of the engagement type (for example, a compliance audit), the level of the auditee (strategic or operational), or the characteristics of the organisation (for example, private sector industry or public sector administration).

The literature identifies the internal audit engagement process as having developed through four generations (McNamee & Selim 1998: 5; Spira & Page 2003: 653–656), namely first (pre-1980s), second (1980s), third (1990s) and fourth (after 2000). Although the word 'risk' is first mentioned in relation to the second-generation internal audit engagements (1980s), it is limited there to financial and compliance risk, and it is only from the 1990s onwards (third and fourth generations) that the concept of risk has been more broadly incorporated into the engagement process. Studies focusing on the current trends within the internal audit profession show that there is growing support for the movement towards auditing more effectively and efficiently (IIARF 2007: 216–233; E&Y 2008: 59; PwC 2008a: 16–19; PwC 2008b: 31–35; IIARF 2009: 9; IIARF 2011: V). From these studies, with topics that include continuous internal auditing and the placing of increasing emphasis on risk, the way forward for modern internal audit engagement planning is increasingly risk based. However, it is still debatable whether all these studies share the same understanding of the concept of risk-based internal auditing. Although all 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 a risk-based internal audit engagement is viewed similarly by all authors. In the next section, definitions of this concept are analysed in order to reach a common understanding of what this concept entails.

Risk-based internal auditing is a fairly new concept for the internal audit profession, and not much has yet been written on the topic. Most of the related research refers to the risk management strategy of the organisation or to the risk-based internal audit function's annual plan. Only a few relevant definitions remain (McNamee & Selim 1998: 199; IIA (UK & Ireland) 2003: 1; Griffiths 2006a: 26; Griffiths 2006b: 9; Spencer Pickett 2006: 205; Spencer Pickett 2010: 225) after discarding the literature

covering organisational risk management strategies and risk-based annual plans. These are summarised as follows:

Firstly, risk-based internal audit engagements are based on a sound risk management process which:

- is implemented by management;
- covers all levels within and across the organisation, such as strategic and operational levels, using an organisation-wide approach; and consists of an output, such as a risk register, that lists all the identified risks.

Secondly, when performing a risk-based internal audit engagement, the internal auditor should ensure that the engagement process:

- treats risk as the primary focus area instead of focusing on conventional areas 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.

The preceding summary indicates that it would be extremely difficult to implement a risk-based internal audit engagement without already having a sound risk management process in place (i.e. a structured process that identifies, assesses and mitigates risks [COSO 2004: 16]), which is indicated by the maturity of the organisation's risk management strategy. The summary identifies a second prerequisite for the implementation of risk-based internal auditing, namely that the outcome of the risk management process or, at the very least, the risk assessment step, must be documented, resulting, for example in a risk register. Thirdly, the risk management process should be performed on and across all possible levels, including the strategic and operational (business unit or process) levels, thus effecting a holistic risk management approach (also referred to as 'organisational' or 'enterprise-wide'), rather than a silo approach. Lastly, although not addressed specifically in the summary, internal auditing should only rely on the outcome of the risk management process as part of the risk-based internal audit engagement after assurance on the risk management process has been obtained; and the risk management process is identified as a sound governance principle (IIA [UK & Ireland] 2003: 2; IOD 2009: 74). These concepts will be briefly explained.

The risk maturity of an organisation is determined by the extent to which a risk management strategy has been planned, adopted and applied by management (De

la Rosa 2008). The more effectively the relevant activities and elements of the risk management strategy have been implemented, the more risk mature the organisation is. The IIA (UK & Ireland) (2003) and experts specialising in risk-based internal audit engagements (Griffiths 2006a: 23; Griffiths 2006b: 15–17; De la Rosa 2008; Baker 2010: 32) are of the opinion that the risk maturity of a specific organisation will play a significant role in how risk management principles can be incorporated into an internal audit engagement. For example, a low level of risk maturity will result in internal auditing performing a risk assessment to determine the scope of the audit engagement, which could be a lengthy and costly approach, while a high level of risk maturity will result in internal auditing providing assurance on the risk management process, and if acceptable, using the outcome of the process to plan the audit engagement.

A risk register, also referred to as the 'risk database', is a document that keeps track of the outcomes of the risk management process within various organisational activities, and is performed on many different levels (Griffiths 2006a: 23; De la Rosa 2008; Campbell 2008: 55–57). The more risk mature the organisation is, the more likely it is that a proper risk register will be kept (Griffiths 2006b: 16; Mutton 2012). Therefore, where 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 literature further mentions that a risk management department should be established and/or a chief risk officer should be appointed to implement the risk management process and to document the outcome of the process (COSO 2004: 86; IOD 2009: 74–75).

Although it seems that for a risk-mature organisation, the risk management principles should be incorporated into the internal audit engagement, it is possible that only strategic risks are determined by management (Griggs 2008: 45; Killackey 2009: 29), and that risks related to specific business units or processes are either not managed or managed within the unit or silo. The danger of this approach is, firstly, that the strategic objectives of the business, being dependent on the achievement of operational objectives, will not be fully achieved. Secondly, it is possible that certain risks are not being properly addressed. Examples of where the failure to manage operational risks has led to fraud and other malpractices (Martin 2009/10: 78-82) include Barings Bank, Citigroup, Société Générale, Northern Rock, HBOS, USB and AIG. When a risk-based internal audit engagement is performed, it is thus a prerequisite that risks have been identified, assessed and managed for the activity under review, whether it is a strategic or an operational-based engagement.

Empirical study

The previous section identified various organisational elements that should be present to enable internal auditors to incorporate risk management principles into the risk-based internal audit engagement. The empirical findings on the existence and use of these elements within organisations are discussed in the following subsections.

Risk maturity

The literature suggests that a risk-based internal audit engagement incorporating risk management principles can only be implemented if an organisation is risk mature. As mentioned in the section on the research methodology, the selection of the five private and five public sector organisations for this study was based on their risk-maturity levels. The risk-maturity levels for the top 40 companies listed on the South African stock exchange, the JSE Limited, as on 8 April 2009, as well as the 37 national departments in the South African government on that date, were calculated and the five organisations per sector with the highest risk maturity were chosen. The Risk and Insurance Management Society (RIMS) model (RIMS 2006) was adapted for South African governance guidance (IOD 2002) and legislation (Public Finance Management Act [PFMA], Act No. 1 of 1999), in which eight attributes were identified (vertical axes of the model), namely culture, strategy setting, risk management policy, risk management process, people, risk management performance, internal auditing and reporting/communication. The risk maturity levels were ranked from level 1 ('ad hoc') to level 5 ('optimised') (horizontal axes of the model), with 40 key performance indicators for the eight attributes per five levels. Each attribute's key performance indicators, based on information available on the Internet and McGregor BFA databases, were ranked for each organisation. The risk-maturity level was calculated by multiplying each level by five, totalling a maximum possible score of 200 (8 attributes x maximum level 5 x 5). Based on the key performance indicators within each level of the eight attributes, risk maturity was determined at level 3, thus totalling 120. In Table 1, the overall risk maturity levels of the ten organisations (all 8 attributes) and their internal audit functions (only the attribute for internal auditing) are provided.

It is clear that the responding organisations from the private sector are much more risk mature than those from the public sector (for all the organisations, 30 of the 40 private-sector organisations and 0 of the 37 public-sector organisations). Risk maturity was measured at >120 (level 3 x 8 attributes x 5), as the key performance indicators within levels 1 and 2 of the RIMS model suggest that very few risk management activities are performed within the eight attributes. Therefore, the public sector

Table 1: Risk maturity levels of responding organisations

	Private sector		Public sector	
	General maturity (total = 200)	Internal audit maturity (total = 5)	General maturity (total = 200)	Internal audit maturity (total = 5)
1	165	4	90	3
2	170	4	95	3
3	170	4	95	3
4	170	5	100	4
5	195	5	100	4

organisations were not included in the section on the performance of a risk-based internal audit engagement. However, it is significant that the risk maturity of internal audit functions in public sector organisations was acceptable (3 and above), thus supporting the choice of chief audit executives as interviewees.

Risk management process and risk register

As discussed in the section on the organisational elements enabling a risk-based approach, the implementation of the risk management process at various levels within organisations, and the documentation of the outcome of the process in a risk register, are two important organisational elements that need to be in place and available to internal auditing to incorporate into the performance of a risk-based internal audit engagement. The risk register should be updated on a regular basis so that the emergence of new risks or any change in the measurement of an existing risk can be properly communicated to all affected parties.

As shown in Table 2, all five of the private-sector organisations surveyed for this research have implemented risk management processes at the strategic and operational levels, and the outcomes of all these processes have been documented in a risk register. However, only two have implemented an integrated, organisation-wide risk management process (holistic approach). In the organisations that do have a risk department headed by a chief risk officer, these departments usually take responsibility for the implementation of the risk management processes at their specific organisational levels. One private sector organisation uses the internal risk steering committee for operational risk management processes.

Table 2: Risk management process: implementation and documentation level

Organisational level	Private sector				Public sector			
	Process	Risk register	CRO	Risk Department	Process	Risk register	CRO	Risk Department
Strategic	5	5	1	4	4	4	3	1
Operational	5	5	1	3	4	4	3	1
Organisation-wide	2	2	1	1	1	1	1	0

CRO = Chief risk officer

Only one responding public sector organisation has not yet implemented a risk management process, and only one responding organisation has implemented an integrated organisation-wide risk management process. For responding public sector organisations that have implemented a risk management process or processes at strategic and/or operational levels, the outcome is documented in a risk register. Only one responding organisation indicated that it has a risk department in place, and that this department takes responsibility for the risk management processes on all the levels. In all the other responding organisations, the chief risk officer takes responsibility for the implementation of the risk management processes at the strategic and operational levels. With regard to 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 all these processes. It is debatable whether one person can take on such an extensive and all-embracing task successfully.

The risk register update frequencies of the responding organisations are listed in Table 3.

Table 3: Frequency of update of the risk register

Frequency	Private sector	Public sector
Continuously	2	0
Monthly	3	2
Biannually	0	0
Less frequently	0	0
Unknown	0	2

For the private sector, three of the responding organisations updated their risk register on a monthly basis, with two responding organisations updating theirs continually. With regard to the responding organisations from the public sector, one had no risk register, while only two updated their risk registers on a monthly

basis. It is, however, a matter of concern that, in the case of two of the public sector organisations, the chief audit executive was not sure of the frequency of updating the risk register.

Involvement of internal auditing

As mentioned previously, although the published research does not specifically mention that the internal audit function should provide assurance on the risk management process in order for the outcome to be incorporated into a risk-based internal audit engagement, it is seen as a sound governance principle. The involvement of the internal audit function in the risk management process was therefore included in the empirical study.

When the degree of adherence to the IIA's formal guidance (IIA 2011) by the ten responding internal audit functions was investigated, all the private sector organisations indicated that the risk management process was evaluated, and that assurance was provided thereon by internal auditing. Three organisations indicated that they were also facilitating the identification and assessment of risks as part of the risk management process. With regard to the public sector, only one responding organisation was adhering to the guidelines on evaluating the risk management process, but all were planning to perform this task in future. Three organisations indicated that they were also facilitating the identification and assessment of risks.

In Table 4, the respondents' views of their organisations' internal audit involvement in the risk management process are categorised.

Table 4: 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 4 is divided into two sections. Above the bold line, the number of responding organisations that include internal audit engagement findings in the organisational risk register is recorded, and below the bold line, the possible roles of internal auditing

in the risk management process are identified, and the number of responding organisations that fulfil them is provided.

All the responding organisations, in both the private and public sectors, that did have a risk register, used the results of internal audit engagements to update the risk register.

When comparing the responding organisations' adherence to the IIA's formal guidance (refer to preceding discussion) on the role of internal auditing in the risk management process, contradictory evidence was obtained. For the private sector, all internal audit functions audit the effectiveness of the process followed, which is in line with their claim of adherence to the IIA guidelines. However, in contrast, the private sector's internal audit functions have no involvement in facilitating the risk management process. For the public sector, three of the respondents indicated that internal auditing has no involvement in the risk management process, while one indicated that internal auditing evaluated the effectiveness of the process, which is in line with the claim of adherence to the IIA guidance as already discussed. However, one internal audit function claimed to assist in facilitating the process, which is in contrast to adherence to the IIA guidance as already mentioned.

It appears that respondents in both the private and public sectors could still be unsure about which duties the internal audit function was actually performing, or, probably more accurately, unsure how to describe the actions and duties being carried out. A further concern was that three of the public sector organisations were performing no risk management process activities.

Planning phase of an internal audit engagement

This section discusses the literature supporting the second research objective, namely whether risk management principles can be incorporated into the planning phase of an internal audit engagement, and if so, how this can be accomplished.

According to the IIA (2011: 16), a plan must be developed and documented for each internal audit engagement that is to be 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. As mentioned before, the planning phase forms the basis upon which the success of the rest of the engagement rests. If the plan is unclear or not comprehensive enough, procedures will not be performed correctly or may even be excluded from the engagement. If, however, the plan is too comprehensive, valuable resources will be unnecessarily deployed, as the internal auditors will perform engagement procedures on areas where they are not needed. Thus, to perform an effective and efficient engagement means that the planning

phase must be carried out with the utmost care. According to IIA *Standard 2200* (IIA 2011: 16–17) and related practice advisories (IIA 2011: 69–70), various aspects must be considered when planning an engagement, most of which are self-explanatory. An area that does need further debate, however, is the inclusion of the concept of risk in the planning of the internal audit engagement. To determine what is required of the internal auditor in this regard, and whether risk management concepts can be used as a basis, the IIA guidance is compared to the risk management process described in the *Enterprise Risk Management Integrated Framework* report (COSO 2004) and summarised in Table 5. This document was chosen for its focus on risk management, suggesting that internal control is one of the risk-mitigating activities (in a risk-driven approach). In contrast, although the Committee of Sponsoring Organisations (COSO) published a previous report, *Internal Control: Integrated Framework* (COSO 1992) and is in the process of updating this document (COSO 2012), both these documents focus on internal control, with risk assessment being nothing more than a step in the development and implementation of appropriate controls (in a control-driven approach).

Table 5: A comparison of engagement planning with the risk management process:

Step in risk management process	Management/Risk Department's responsibilities (COSO 2004)	Internal audit engagement planning considerations (IIA 2011)
Objective setting	• Development of objectives and criteria	• Consider activity's objectives and criteria • Develop activity criteria if none exist • Develop engagement objectives and scope to address risk areas
Identification of risks	• Identification of significant risks • Risk in related areas (holistic)	• Consider all relevant exposures
Assessment of risks	• Assessment of risks • Monitoring, reporting and resolving risk aspects • Impact of risk within acceptable level (risk appetite) • Reporting 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 where risk exceeds risk appetite • Keeping the impact of risk within an acceptable risk level	• Consider management's report and response where risks exceed risk appetite (potential critical control aspects)
Risk communication and monitoring	• Adequate and effective process	• Consider management's processes on report and monitor risk aspects

The comparison highlights a number of significant facts. Firstly, it is important to note that the IIA recognises that without management's performing certain activities (refer to activities in column 2 of Table 5), the planning of a risk-based internal audit engagement is difficult. Secondly, when it comes to risk, the IIA guidance expects internal auditors to plan their engagements based on the same steps as the risk management process performed by management. This implies that if the risk management process is well performed and properly documented, the internal auditor could use the outcome of the risk management process as the starting point for planning the risk-based internal audit engagement. The question remains whether this tendency to rely on the risk management process is applied in practice. After a search of the Internet and various research databases, only a few relevant studies were identified. These are discussed in the context of either a control-driven or a risk-driven approach.

According to unpublished studies and to specific organisations' processes where a risk-based approach to internal audit engagement is referred to, these only incorporate the risk assessment step in order to identify appropriate controls, thus identifying this as a control-driven approach, as discussed above (McNamee & Selim 1998; Bank of Canada 1998; Spencer Pickett 2003; Deloitte 2005; Spencer Pickett 2006; Sobel 2008; Clayton 2009). Specific tendencies that should be mentioned include that risk analyses are not performed (McNamee & Selim 1998: 103–105; Spencer Pickett 2003: 402; Clayton 2009: 35–39); that only the controls that mitigate the risks must be included in the audit engagement (McNamee & Selim 1998: 106; Deloitte 2005: 7); that no integration of controls and risk assessment is being performed (Spencer Pickett 2003; Sobel 2008: 93); that internal auditing performs their own risk assessment as part of the audit engagement (Spencer Pickett 2006: 143–161; Sobel 2008: 93); and that the focus is only on financial risks (Deloitte 2005: 1–10). Although there are literature studies that support the risk-driven approach, as discussed above (Griffiths 2006a; Griffiths 2006b; Pelletier 2008; Reding, Sobel, Anderson, Head, Ramamoorti, Salamasick & Riddle 2009), the following weaknesses in their arguments were identified:

- Internal auditors perform their own risk assessment based on the objectives of the activity under review. If risk assessment from the formal risk management process is used, duplications will be eliminated. However, as previously discussed, this will only be possible if the organisation is risk mature, and if the risk management process has been audited by the internal audit function and found to be reliable.
- Previously, the term 'risk' referred mainly to hazards (Prinsloo 2008: 216–226). The modern approach to risk includes the loss of opportunity (COSO 2004: 16). It seems that this concept is still not being included in the risk-based internal audit engagement planning process.

- According to the risk management process, the difference between an inherent risk (i.e. the possibility of an event occurring that could cause harm to an organisation in the absence of any preventative, corrective or detective measures) and a residual risk (i.e. the remaining risk after mitigating activities have been implemented) is the existence of current responses that have been put in place to mitigate the risk to an acceptable level (COSO 2004: 49–54). The movement between these two levels of risk should thus provide internal auditors with a starting point when planning the engagement procedures. However, it seems that this is not currently the case.
- As previously discussed, risk cannot be viewed in silos but has to be viewed holistically (COSO 2004: 15). With reference to an internal audit engagement, this could mean that a risk identified in a particular business unit or process might have an impact on another. The internal auditor should review the effect of these risks on the whole organisation instead of only on the smaller unit.
- It seems that controls are mostly investigated as a means of reducing risks. Other mitigating procedures or risk responses, such as sharing the risk (COSO 2004: 55–66), are not mentioned but could be more appropriate or cost-effective.

Apart from these weaknesses in performing a risk-based internal audit engagement based on the risk management principles, the internal audit engagement process used, as identified in much of the literature, still refers to the control-driven process, even though it should be risk driven, based on the internal audit generation (refer to the discussion in the section on organisational elements enabling a risk-based approach), as reflected in the literature sources (Spencer Pickett 2003; Deloitte 2005; Spencer Pickett 2006; Sobel 2008; Clayton 2009). It seems that although some individuals and organisations promote the performance of risk-based internal audit engagements based on risk management principles, and more specifically the process documented in the 2004 COSO Report, there are still several gaps that prevent the utilisation of the process to its fullest potential.

Empirical study

As stated in the subsection on risk maturity, only the private sector participated in this part of the research due to the low risk maturity of the public sector's responding organisations. This section consists of a discussion of the performance of an internal audit engagement based on risk management principles, including the starting point and how information is obtained during the planning phase, and the weaknesses

that need to be addressed to incorporate risk concepts fully into risk-based internal audit engagements.

Internal auditing and risk management processes

Table 5 links modern internal audit engagement planning to the risk management process as documented in the COSO Report of 2004 (which refers to a risk-driven approach). However, the literature supports the perception that a control-driven approach, as documented in the COSO Report of 1992, is more frequently used when referring to a risk-based internal audit engagement. Respondents were asked to identify the approach that they followed when performing risk-based internal audit engagements (refer to Table 6 – Before). The difference between these two approaches was then explained to respondents, after which they were invited to re-evaluate their view of the approach they were currently following (refer to Table 6 – After).

Table 6: Process used during internal audit engagements

Control driven (COSO 1992)		Risk driven (COSO 2004)		Other		Not sure	
Before	After	Before	After	Before	After	Before	After
2	3	2	1	1	1	0	0

The results indicate that during engagements, the respondents could link their internal audit process to either the control-driven (COSO 1992) or the risk-driven (COSO 2004) approach, with only one respondent suggesting that their self-developed process was a combination of the two approaches. After the application of the two approaches in an internal audit engagement had been explained to respondents, one organisation came to the realisation that their process followed the control-driven approach more closely than it did the risk-driven approach as initially perceived by the chief audit executive. It was also noted that two responding organisations were still using the old process when performing risk-based internal audit engagements.

Starting point during planning

Although the two approaches both focus on the incorporation of risk management principles into the internal audit engagement as their starting point, the risk-driven approach focuses on the difference between the inherent and residual risk ratings for each individual risk. Table 7 provides information on the various methods organisations use when planning their engagements.

Table 7: Elements used as the starting point of the planning phase

Previous year's working papers	Inherent risks as per the risk register	Di erence between the inherent and residual risks as per the risk register
4	5 (3 + 2)	4 (2 + 2)

Respondents were asked to identify all the elements used by their internal audit functions during the planning phase of an internal audit engagement. The results indicated that the element that was incorporated into the planning phase of an internal audit engagement was always management's measurement of the inherent risks (refer to the second column of Table 7). Two of the respondents indicated that, although they had considered this element as well as management's assessment of the inherent and residual risks (refer to the third column of Table 7), they relied more on the outcome of their own risk assessment (refer to Annexure A, question 7.3 'Other'). Taking all these discussions into considerations, it could be concluded that the previous year's working papers were the most commonly used planning aid, as four of the five organisations always used this resource.

Information obtained

In Table 5, the steps in the risk management process were analysed to determine how the various steps are treated in the planning phase of an internal audit engagement. In Table 8, the practical implementation of these steps is analysed.

Table 8: Key steps of the risk-based internal audit engagement planning

Key steps	Use auditee input	Use risk management process results (risk register)	No/limited information (internal auditor has to obtain)
1. Operational (auditee) objective setting	4	5	4
2. Risk identification for inherent risks	2	5	2
3. Risk assessment (measure) for inherent risks	1	5	2
4. Current risk-mitigation activities	2	3	5
5. Risk assessment (measure) for residual risks	0	4	3

The results indicate that most of the respondents used the risk register to obtain the auditee's objectives, after which it was used to identify inherent risk and, lastly, to obtain the assessment of the risks. Additional information was gathered either

by obtaining the auditee's input or through the internal auditor performing certain tasks. This is in line with the results provided in Table 7 on the inherent risks as a starting point for the planning phase and the two respondents indicating that they also perform their own assessment.

It appears that internal auditors prefer to rely on their own interpretation to determine whether the current mitigation activities are in place (key step number 4), with all five respondents indicating that internal auditors had obtained this information with limited input from the auditee (two respondents) and the risk register (three respondents). However, the respondents indicated that they then relied on the risk register (four respondents) for the residual risk assessment (key step number 5). The assessment of the residual risk assessment is dependent on the current risk-mitigation activities already in place, 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 (one respondent).

Underdeveloped areas

During the literature study, five weaknesses or underdeveloped areas were identified when a risk-driven approach was followed in performing an internal audit engagement. The first area (internal auditors prefer to perform their own risk assessment) and the third area (the difference between the inherent risk and the residual risks should be the starting point during planning) have been covered in the previous discussion (refer to Table 8). The remaining three areas are addressed in Table 9.

Table 9: Underdeveloped areas in a risk-based internal audit engagement

Both threats and loss of opportunities are identified	E□ect of risk in engagement on another area	E□ect of another risk on current engagement	Recommend other risk-mitigating activities (not controls)
4	5	5	2

All five respondents indicated that they reflect on the effect of risks on other areas and *vice versa*. The results referring to the integrated organisation-wide risk management strategy (refer to the second and third columns of Table 9) contradict the results in Table 2. The responses reported in Table 2 indicated that only two organisations have an integrated organisation-wide risk management process in place and document results in the risk register. It is important to note the last weakness (refer to column 4 of Table 9), namely that internal auditors are reluctant to recommend risk-mitigating activities other than controls.

Further comments by respondents on the risk-based planning of internal audit engagements included the use of computer-assisted audit techniques to facilitate the identification and assessment of risks; the view that the risk department's systems were not mature enough to allow the internal audit function to perform a risk-driven internal audit engagement; and acknowledgement that risks were still being treated within silos instead of organisation-wide integrated risk-mitigation efforts.

Conclusion

Internal auditing is entering a new phase due to the rapid growth of the scope and nature of its responsibilities, and demands from various stakeholders for effective and accurate assurance. The profession needs a new mindset with respect to the way internal audit activities are performed, accompanied by new methodologies. A comparison of the steps in the internal audit engagement process with those in the risk management process introduces a new way of performing an engagement, referred to as risk-based internal audit engagement. Supported by both the literature and the views of the chief audit executives interviewed, it seems that the term 'risk-based internal auditing' is fairly new, in that the terminology is not only used inconsistently, but is sometimes used to describe the audit of the risk management strategy as well as the development of the internal audit function's annual plan. A common understanding of the term will emerge when organisations are risk mature, have a risk management process and a formal risk register in place, and follow a holistic or enterprise-wide approach to risk management. Further analysis of the literature on the process used in practice indicates that not all the elements of the risk management process are fully integrated, and that further improvements to streamline the internal audit engagement process are needed. These should be included in a position paper from the IIA on risk-based internal auditing.

The empirical study on which this article is based indicated that the majority of private sector organisations are risk mature (30 of 40 listed companies met the criteria), usually have an organisation-wide risk management process in place, and document the outcome of the process in a regularly maintained risk register. By contrast, public sector organisations are risk immature (0 of 37 national departments met the criteria), and have risk management processes predominantly for their strategic and operational processes/units. All the empirical findings should be interpreted against this fact. Furthermore, it became obvious that organisations still need to be made aware of tools such as the RIMS risk-maturity model, which could assist them in understanding risk maturity in general, their own levels of risk maturity, and what is needed for their organisations to reach the desired maturity level.

With regard to the findings identifying the organisational elements supporting risk-based internal audit engagements and the planning phase of an internal audit engagement, a tendency that is of concern is that some of the chief audit executives are unsure how frequently the risk register is being updated with emergent risks, which could compromise the relevance of the internal audit function's activities. Respondents from both sectors indicated that internal auditing is involved in the risk management process. However, when asked whether the function complied with the IIA's guidance on this topic, the answers were contradictory. This could be an indication that even chief audit executives are unsure of the various terminological differences, and the diversity of activities and roles in respect of risk management and risk-based internal auditing. This was supported by the fact that respondents in the private sector were either unsure of the type of risk management principles incorporated in the internal audit engagement process, or still used the control-driven process. Further indications that internal auditors are not using a risk-driven internal audit process are their preference for using the previous years' working papers as a starting point for the planning phase, and the on-going reliance on the auditee's input, or on internal auditors' performing tasks to obtain information that should have been obtained from the risk register.

It seems that internal auditors are still unclear about the differences between risk management and risk-based internal auditing in terms of their respective terminologies, methodologies and roles. They also appear uncertain how to include risk management principles in the planning of an internal audit engagement. It could be argued that this is a normal situation when a new concept is introduced. The use of interviews as part of the empirical study limited the distortions that these uncertainties might otherwise have introduced to the research results, as terminologies were explained and the interviewer tried to ensure that all interviewees had the same idea of each specific concept. It is recommended, however, that the IIA develop a position paper that clarifies these aspects, not only for internal auditors, but for the business world in general. This will provide greater understanding of the contribution that internal auditors could make to the mitigation of key risks. Mervyn King, chairman of the King Committee (cited in Baker 2010: 31) declares that internal auditing is "the right arm of the non-executive board". This statement explicitly acknowledges that the IIA, as a professional body, has the ability to beneficially influence many others.

References

Baker, N. 2010. 'Equipped for governance', *Internal Auditor*, 67(1): 29–32.

Bank of Canada. 1998. *Risk-based Internal Auditing and Dynamic Control Assessment: Revolutionising Internal Audit Services*. Altamonte Springs, FL: Institute of Internal Auditors.

Campbell, T. 2008. 'Risk management: Implementing an effective system', *Accountancy Ireland*, 40(6): 54–57.

Castanheira, N. Rodrigues, L.L. & Craig, R. 2010. 'Factors associated with the adoption of risk-based internal auditing', *Managerial Auditing Journal,* 25(1): 79–98.

Clayton, D. 2009. 'A risk-centric approach that works', *Internal Auditor*, 66(1): 35–39.

COSO (Committee of Sponsoring Organisations of the Treadway Commission). 1992. *Internal Control – Integrated Framework: Framework*. Jersey City, NJ: Sponsoring Organisations of the Treadway Commission.

COSO (Committee of Sponsoring Organisations of the Treadway Commission). 2004. *Enterprise Risk Management Integrated Framework: Executive Summary*. Jersey City, NJ: Jersey Sponsoring Organisations of the Treadway Commission.

COSO (Committee of Sponsoring Organisations of the Treadway Commission). 2012. COSO develops draft update to internal control-integrated framework and related supporting documents. [Online] Available from: http://www.coso.org. Accessed: 21 August 2012.

De la Rosa, S. 2008. *How to Effectively Review your Organisation's Risk Management Process*. Johannesburg: Institute of Internal Auditors Training Program.

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.

E&Y (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.

FASSET (Finance, Accounting, Management Consulting and other Financial Services Sector Education and Training Authority [SETA]). 2011. *FASSET Scarce Skills Guideline: February 2011*. [Online] Available from: http://www.fasset.org.za/downloads/research/SS_Guide-_2011_V4.pdf. Accessed: 26 July 2011.

Griffiths, D. 2006a. *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. 2006b. *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', *RMA Journal,* 90(9): 44–49.

Hamid, E. 2012. 'The application of analytic hierarchy process for risk-based allocation of internal audit resources', *Advances in Asian Social Science,* 1(4): 343–345.

IOD (Institute of Directors). 2002. *King Report on Corporate Governance for South Africa*. Johannesburg: King Committee on Corporate Governance.

IOD (Institute of Directors). 2009. *King Report on Governance for South Africa*. Johannesburg: King Committee on Corporate Governance.

IIA (Institute of Internal Auditors) (UK and Ireland). 2003. Position statement: Risk based internal auditing. [Online] Available from: http://www.iia.org.uk. Accessed: 14 March 2007.

IIA (Institute of Internal Auditors). 2011. *International Professional Practices Framework*. Altamonte Springs, FL: Institute of Internal Auditors.

IIARF (Institute of Internal Auditors Research Foundation). 2007. *CBOK (A Global Summary of the Common Body of Knowledge 2006)*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

IIARF (Institute of Internal Auditors Research Foundation). 2009. *Knowledge Alert: 2009 Hot Topics for the Internal Audit Profession*. Altamonte Springs, FL: Global Audit Information Network, Institute of Internal Auditors Research Foundation.

IIARF (Institute of Internal Auditors Research Foundation). 2011. *CBOK: What's Next for Internal Auditors?* Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Killackey, H. 2009. 'Integrating enterprise risk management with organisational strategy', *RMA Journal*, 91(8): 28–35.

Koutoupis, A.G. & Tsamis, A. 2009. 'Risk based internal auditing within Greek banks: A case study approach', *Journal of Management and Governance*, 13(1–2): 101–130.

Lemon, W.M. & Tatum, K.W. 2003. *Research Opportunities in Internal Auditing: Internal Auditing's Systematic and Disciplined Process*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Martin, P.H. 2009/10. 'As risk management evolves, is operational risk management important?', *Journal of Operational Risk*, 4(4): 75–84.

McNamee, D. & Selim, G.M. 1998. *Risk management: Changing The Internal Auditor's Paradigm*. Altamonte Springs, FL: Institute of Internal Auditors.

Mutton, J. 2012. Do I really need a risk register? [Online] Available from: http://search.informit.com.au/documentSummaru:dn=728781013590067:res=IELBUS. Accessed: 8 September 2012.

Pelletier, J. 2008. 'Adding risk back into the audit process', *Internal Auditor,* 65(4): 73–76.

Prinsloo, J. 2008. The development and evaluation of risk-based approaches. Unpublished MCom (Accounting) dissertation. University of the Free State.

PwC (PricewaterhouseCoopers). 2008a. Targeting key threats and changing expectations to deliver greater value. [Online] Available from: http://www.PwC.com/extweb/PwCpubli-cations.nsf/docid/state_internal_audit_profession_study_08.pdf. Accessed: 3 May 2008.

PwC (PricewaterhouseCoopers). 2008b. 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.

PwC (PricewaterhouseCoopers). 2012. Aligning internal audit: State of the internal audit profession study [Online] Available from: http://www.PwC.com/en_US/us/risk-assurance-services/internal-audit/publications/assets/PwC-2012-state-of-internal-audit-survey.pdf/. Accessed: 10 September 2012.

Reding, K.F., Sobel, P.J., Anderson, U.L., Head, M.J., Ramamoorti, S., Salamasick, M. & Riddle, C. 2009. *Internal Auditing: Assurance and Consulting Services* (2nd edition). Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

RIMS (Risk and Insurance Management Society) 2006. RIMS risk maturity model for enterprise risk management. [Online] Available from: http://www.rims.org/rmm. Accessed: 12 March 2009.

Sobel, P. 2008. 'Risk management-based auditing', *Internal* Auditor, 65(4): 92–93.

Soh, D.S.B. & Martinov-Bennie, N. 2011. 'The internal audit function: Perceptions of internal audit roles, effectiveness and evaluation', *Managerial Auditing Journal*, 26(7): 605–622.

SAICA (South African Institute of Chartered Accountants). 2009/10. *SAICA Handbook*, Vol. 2. South Africa: LexisNexis.

Spencer Pickett, K.H. 2003. *The Internal Auditing Handbook* (2nd edition). New Jersey: Wiley & Sons.

Spencer Pickett, K.H. 2006. *Audit Planning: A Risk-based Approach*. New Jersey: Wiley & Sons.

Spencer Pickett, K.H. 2010. *The Internal Auditing Handbook* (3rd edition). West Sussex: Wiley & Sons.

Spira, L.F. & Page, M. 2003. 'Risk management: The reinvention of internal control and the changing role of internal audit', *Accounting, Auditing and Accountability Journal*, 16(4): 640–661.

Annexure A

Structured interview schedule

1. **Organisational background(*)**
2. **IIA Standards**

<table>
<tr><td rowspan="3">2.1</td><td colspan="6">Does the IAF adhere to the IIA Standards?</td></tr>
<tr><td colspan="2">Always</td><td colspan="2">Most of the time</td><td colspan="2">Never</td></tr>
<tr><td colspan="6">If ‘most of the time’, which broad area(s) are not covered?</td></tr>
<tr><td colspan="7">Provide reasons for why all areas are not covered:</td></tr>
<tr><td rowspan="5">2.2</td><td colspan="7">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>Activity</td><td colspan="3">Adherence</td><td colspan="2">More guidance</td></tr>
<tr><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>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>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>
</table>

3. **The changing** internal audit environment(*)
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.)
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.)

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 requently	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 involvement	Audit the effectiveness of the process methodology		Audit the results of the process	Facilitates the process	Takes partial responsibility for the process	Takes full responsibility for the process	Other	
	If 'other' involvement, indicate:								

6. Annual planning of the IAF's activities(*)

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 1992 model terminology		Yes	No	Not sure
	COSO 2004 model terminology		Yes	No	Not sure
	If another methodology is used, indicate:				
7.2	If using the COSO1992 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 (*)

(*) Not included for the purposes of this study