INTOSAI

Guidelines for Internal Control Standards for the Public Sector

Further Information on Entity Risk Management

INTOSAI GOV 9130

INTOSAI PSC Subcommittee on Internal Control Standards

2007

INTOSAI Internal Control Standards Subcommittee

F. VANSTAPEL
Senior President of the Belgian Court of Audit

Regentschapsstraat 2 – Rue de la Régence 2
B-1000 BRUSSELS
BELGIUM

Tel : + 32 2 551 8111
Fax : + 32 2 551 8629
E-mail : international@ccrek.be

Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management

Preface

The 1992 INTOSAI *Guidelines for Internal Control Standards* were conceived as a living document reflecting the vision that standards should be promoted for the design, implementation, and evaluation of internal control. This vision involves a continuing effort to keep these guidelines up-to-date.

The 17th INCOSAI (Seoul, 2001) recognized a strong need for updating the 1992 guidelines and agreed that the Committee on Sponsoring Organisations of the Treadway Commission's (COSO) integrated framework for internal control should be relied upon. Subsequent consultation resulted in a further expansion to address ethical values and provide more information on the general principles of control activities related to information processing.

The updated Internal Control Guidelines were issued in 2004 and should also be viewed as a living document

which over time will need to be further developed and refined to embrace the impact of new developments such as COSO's Enterprise Risk Management *framework*[1]. Accordingly, this addition to the Guidelines has been produced to cover current thinking on risk management, as set out in COSO's *ERM framework*. As this paper is intended primarily for public sector readers the term "entity" is used in place of "Enterprise" which has a particular private sector association.

The additional information provided here is the result of the joint effort of the members of the INTOSAI Internal Control Standards Subcommittee. This update has been coordinated by a Task Force set up among the subcommittee members with representatives of the SAIs of France, Hungary, Bangladesh, Lithuania, the Netherlands, Oman, the Ukraine, Romania, the United Kingdom, the United States of America and Belgium (chair).

Franki VANSTAPEL
Senior President of the Belgian Court of Audit
Chairman of the INTOSAI Internal Control Standards Subcommittee

[1] Enterprise Risk Management - Integrated Framework (COSO - September 2004)

Introduction

The underlying premise of the *COSO Entity Risk Management* framework is that every entity exists to provide value for its stakeholders. In the public sector, general expectations are that public servants should serve the public interest with fairness and manage public resources properly. Effectively the stakeholders are the public and their elected representatives.

All entities face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to obtain best value for stakeholders. It is also important to note that uncertainty presents both risk and opportunity, with the potential to erode or enhance value or, in public sector terms to service the public interest more or less well. The aim of entity risk management is to enable management to effectively deal with uncertainty and its associated risk and opportunity, enhancing the capacity to build value, to deliver more effective services more efficiently and economically, and to target them whilst taking into account values such as equity and justice.

The INTOSAI *Guidelines for Internal Control Standards for the Public Sector* sees internal control as providing an overarching conceptual framework through which an entity can be managed to achieve its objectives. The *COSO ERM* framework and other similar models take this a stage further in that the entity can be directed on the basis of identifying future risks and opportunities to refine objectives and design internal controls to minimise risk and maximise opportunity.

As well as extending the definition of functions covered by the corporate governance regime entity risk management required a change in the way organisations think about achieving their objectives. This is because to be effective,

entity risk management is an ongoing process applied in strategy setting, effective across and affected by all levels and every business unit of an entity and which is designed to identify all events that will affect the organisation's ability to achieve its objectives.

This document outlines a recommended framework for applying the principles of entity risk management in the public sector and provides a basis against which entity risk management can be evaluated. However, it is not intended to replace or supplant the *Guidelines for Internal Control Standards for the Public Sector* but rather is designed to provide complementary additional information to be used alongside those standards where member states consider it to be appropriate to do so. Nor, is it intended to limit or interfere with duly granted authority related to developing legislation, rule-making or other discretionary policy-making in an organisation.

In conclusion, it should be clearly stated that this document includes additional guidelines for corporate governance standards. The guidelines do not provide detailed policies, procedures and practices for implementing a best practice corporate governance regime, nor are they expected to be suitable for all organisations in all regulatory environments. However, the addendum provides an addition to the broad framework within which entities can develop regimes to best help them maximise the services provided to stakeholders.

How is this document structured?

The supplement is structured in a similar manner to the INTOSAI *Guidelines for Internal Control Standards for the Public Sector*. In the first chapter the concept of Entity risk management is defined and its scope is delineated. In the second chapter the components of Entity risk management are presented and the extensions to the internal control standards highlighted.

Chapter 1: What is Entity Risk Management

1.1 Definition

1.1.1 COSO's *Entity Risk Management: Integrated Framework* states that Entity risk management deals with risks and opportunities affecting value creation or value preservation defined as follows:

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

1.1.2 In the public sector the terms value creation and value preservation do not have as much direct relevance as in the private sector. However, the definition is purposefully broad to cover as many sectors and types of organisations as feasible. As such it is possible to substitute service creation and preservation for value creation and preservation for the definition to be fully applicable to public sector entities.

1.2 Identifying the Mission

1.2.1 The starting point for Entity risk management is the entity's established mission or vision. Within the context of this mission, management should establish strategic objectives, select strategies to achieve these objectives and set supporting aligned objectives that are cascaded throughout the organisation.

1.3 Setting Objectives

1.3.1 The INTOSAI Guidelines on Internal Control Standards states that objectives can be sub-divided into four categories (although most objectives will fall into more that one category). These are:

- **Strategic** - high level goals, aligned with and supporting the entities mission
- **Operational** – executing orderly, ethical, economical, efficient and effective operations; and safeguarding resources against loss, misuse and damage
- **Reporting** - reliability of reporting including fulfilling accountability obligations
- **Compliance** - compliance with applicable laws and regulations and being able to act in accordance with Government policy

1.3.2 Objectives in the first two categories are not entirely within an entity's control so any risk management system can only provide reasonable assurance that these risks are being managed

satisfactorily, but should enable management to be aware of the extent to which these objectives are being met in a timely fashion. However, objectives relating to reliability of reporting and compliance are within an entity's control so effective Entity risk management will usually give management assurance that these objectives are being met.

1.4 Identifying Events - Risks and Opportunities

1.4.1 Once objectives have been set Entity risk management requires an organisation to identify events that might have an impact on the achievement of those objectives. Events can have a negative impact, a positive impact or both. Events with a negative impact represent risks, which can hinder the entity's ability to achieve its objectives. These risks can arise due to internal and external factors. Figure 1, below, sets out many of the risks which government entities face – there may well be other risks relevant to particular entities.

1.4.2 Events with a positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur that will enhance the entity's ability to achieve its objectives or enable the entity to achieve objectives more efficiently. As well as seeking to mitigate risks management should formulate plans to seize opportunities.

1.5 Communication and Learning

1.5.1 Determining whether an entity's Entity risk management is "effective" is a fundamental part of the process. Management need to make a judgement on whether the components of Entity risk management are present and operating effectively; namely that there are no material weaknesses and that all risks have been brought within acceptable parameters given the entity's risk appetite. Where Entity risk management is effective management will understand the extent to which objectives in all four categories are aligned with the mission and are being achieved. Effective top down and bottom up communication throughout the entity is essential to facilitate this process.

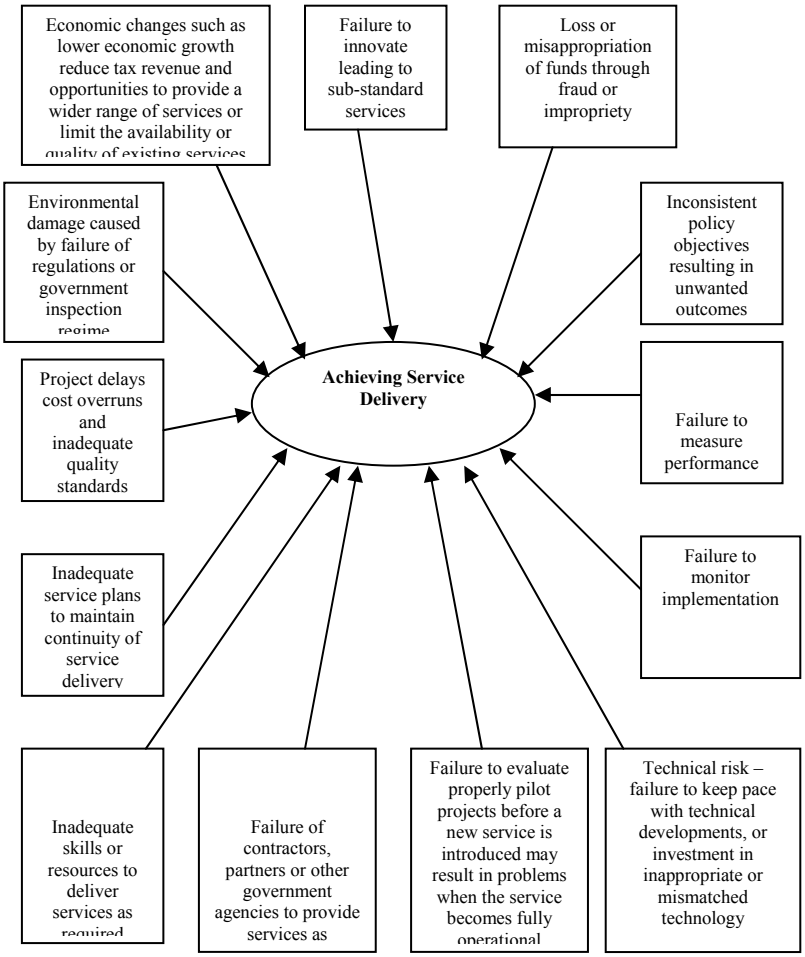
1.6 Limitations

1.6.1 No matter how well designed and operated the system is, Entity risk management cannot provide management with absolute assurance regarding the achievement of general objectives. Instead, this supplement recognises that only a reasonable level of assurance is obtainable.

1.6.2 Reasonable assurance equates to a satisfactory level of confidence that objectives will be achieved or that management will be made aware in a timely fashion if objectives are unlikely to be achieved. Determining how much assurance is required to reach a satisfactory level of confidence is a matter of judgement. In exercising that judgement management will need to consider the entity's risk appetite and events that may impact on achievement of objectives.

1.6.3 Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no-one can predict with certainty. In addition, factors outside an entity's control or its influence, such as political factors, can impact on its ability to achieve its objectives. In the public sector, factors outside an entity's control can even change core objectives at quite short notice. Limitations also result from the following realities: that human judgement in decision making can be faulty; that breakdowns can occur because of human failures such as simple errors or mistakes; that decisions on responding to risk and establishing controls need to consider the relevant costs and benefits; and that controls can be circumvented by collusion between two or more people and management can override the control system. These limitations preclude management from having absolute assurance that objectives will be achieved. Figure 1 sets out some of the risks might typically face. It is intended to be illustrative rather than exhaustive.

Figure 1: Some Typical Risks that Government Entities Face?



1.7 Link between Internal Control and Entity Risk Management

1.7.1 In many respects entity risk management may be regarded as a natural evolution of the internal control model. Most organisations will seek to fully apply the internal control model before implementing the concepts inherent within Entity risk management. Internal control is an integral part of entity risk management. The entity risk management framework encompasses internal control, but in addition, forms a more robust conceptualisation of how an entity's business decisions should fall out of its core mission and associated objectives and provides a tool for management to help them to determine what the correct response to a particular event should be. The ERM model goes further than the INTOSAI Internal Control Guidelines in a number of areas, in particular:

- the categories of objectives are broader, and also include more complete reporting, non-financial information, strategic objectives;
- it expands the risk assessment component and introduces different risk concepts, such as risk appetite, risk tolerance, risk response; and
- it emphasises the importance of independent directors on the board and elaborates on their roles and responsibilities.

Chapter 2:

Components of Entity Risk Management

Entity risk management consists of eight interrelated components. These are derived from the way that management runs a business and are integrated with the management process. The components are:

- Internal environment
- Objective setting
- Event identification
- Assessing risks
- Risk response
- Control activities
- Information and communication
- Monitoring

In applying the components of Entity risk management, an entity should consider the entire scope of its activities at all levels of the organisation. Management should also consider new initiatives and projects using the Entity risk management framework.

Applying Entity Risk Management across the Entity

Management is required to take a portfolio view of risk. In effect all levels of management will need to consider the events that may impact on their areas of activity and feed them up to senior management. This assessment can be qualitative or quantitative. Senior management should use these assessments running through all levels and business areas of the entity to build up an entity level assessment of the overall risk portfolio of the organisation.

Importance of People

Entity risk management is implemented and made to work effectively by an entity's management and other personnel. It is accomplished by what individuals within an organisation do and say. Similarly, Entity risk management affects people's actions. Each employee is an individual with different competencies and understanding. Entity risk management seeks to provide the mechanisms to enable members of staff to understand risk in the context of the entity's objectives.

Members of staff should know their responsibilities and the limits of their authority. Accordingly a clear and concise linkage needs to exist between an individual's duties and the way that they are carried out. Senior management primarily provide oversight. However, they also provide direction, approve strategies and approve certain transactions and policies thereby playing a vital role in enforcing organisational culture.

2.1 Risk Environment/Context

2.1.1 The risk environment/context encompasses the tone of an organisation, influencing the risk consciousness of all of its people and, is the basis for all other components of Entity risk management, providing discipline and structure. Internal environment factors include an entity's risk management philosophy; its risk appetite; oversight by the management board; integrity and ethical values; competence of staff; and the way management assigns authority and responsibility and organises and develops staff.

2.1.2 An entity's risk management philosophy is the set of shared beliefs and attitudes which set out how the entity considers risk in everything it does from strategy setting to day to day operational activities. It influences culture and operating style including how risks are identified, the kind of risks accepted and how they are managed. An entity's risk management philosophy should be captured in policy statements, oral and written communications to stakeholders and staff and in decision making. Irrespective of the method of communication it is of critical importance that senior management reinforce the philosophy, not only through communicating policies, but through everyday actions.

2.1.3 Risk appetite is the amount of risk on a broad level that an entity is willing to accept in seeking to achieve its objectives. It reflects the risk management philosophy and in turn influences the entity's culture and operating style. Risk appetite can be considered quantitatively or qualitatively. It should be considered in strategy setting, where the desired return from a strategy

should be aligned with the risk appetite, that is the willingness to accept or tolerate risk.

2.1.4 In addition, when identifying the risk environment and selecting an appropriate risk appetite, public sector entities need to consider the "extended Entity". The opinions and expectations of sponsoring and sponsored organisations, be they other government bodies or legislation setters, and the opinions of partner organisations can give a clear steer as to a suitable risk management philosophy and risk appetite.

2.1.5 An entity's senior management is a critical part of the internal environment and significantly influences its elements. It is a truism that organisational culture can be set or be fatally undermined by the "tone at the top". The senior management's independence from executive management, experience and stature of members, extent of involvement and scrutiny, and the appropriateness of its activities all play a role. Members of top executive management can be part of senior management, but for the internal environment to be effective it is advisable that the senior management team contain some independent outside members. This is because senior management must be prepared to hold executive management to account by questioning and scrutinising activities and being prepared to present alternative views.

2.1.6 Management's integrity and ethical values influence the way strategy and objectives are implemented. Because an entity's good reputation is so valuable, the standards of behaviour must go beyond mere compliance with

minimum legal standards. Ethical behaviour and management integrity are by-products of corporate culture, which includes ethical and behavioural standards and how this is communicated and enforced. Top management plays a key role in determining the corporate culture. An undue emphasis on short term results as opposed to achieving the overall mission can foster an inappropriate internal environment.

2.1.7 Formal codes of conduct are important to and the foundation of the promotion of an appropriate ethical tone. Upward communication channels (or formal whistleblowing procedures) where employees feel comfortable bringing relevant information to the board are also important. However, a written code of conduct does not by itself ensure that procedures are being followed, even if all employees have to evidence that they are aware of the behaviours expected of them. Equally important to compliance are resulting penalties to employees who violate the code. Messages sent by senior management quickly become embodied in corporate culture, so "doing the right thing" when faced with tough business decisions quickly become embodied throughout the entity.

2.1.8 Competence reflects the knowledge and skills needed to perform assigned tasks. It needs to be supported by human resources practices pertaining to employing and promoting appropriate individuals, induction, training and dealing with poor performance. Management needs to specific competency levels for particular tasks and translate those into appropriate job descriptions for specific posts. It is important to

recognise that a trade-off can exist between competence and cost.

2.1.9 An entity's organisational structure provides the framework to plan, execute, control and monitor its activities. The organisational structure adopted will be suitable to business needs. Some are centralised, others decentralised, some organised by geographical location and others by function. Whatever the structure, an entity should be organised to enable effective risk management and to carry out its activities so as to achieve its objectives.

2.1.10 Assignment of authority and responsibility involves the degree to which individuals and teams are authorised to and encouraged to use initiative to address issues and solve problems as well as the limits to their authority. The key challenges are to ensure that all personnel understand the entity's objectives and how their actions contribute to the achievement of those objectives and only to delegate to the extent required to achieve objectives. Responsibility is as important as authority. The internal environment is greatly influenced by the extent to which individuals recognise they will be held accountable. This holds true all the way to the chief executive.

2.2 Objective Setting

2.2.1 Objectives are set at a strategic level, establishing a basis for lower level operations, reporting and compliance objectives. Every entity faces a variety of risks from external and internal sources and a precondition to effective event

identification, risk assessment and risk response is the establishment of objectives. Objectives must be established before management can identify and assess risks to their achievement and take the necessary actions to mitigate those risks. Objectives are aligned with an entity's risk appetite, which drives risk tolerance levels for the entity.

2.2.2 An entity's mission sets out in broad terms what the entity aspires to achieve. Management sets strategic objectives formulates strategy and establishes related operations. Strategic objectives are high-level goals aligned with and supporting the entity's mission. The strategy implemented to achieve the mission and the related objectives tend to be more dynamic than the mission and will be adjusted to take account of changing conditions.

2.2.3 Despite the diversity of objectives across entities, there are certain broad categories that can be applied. All objectives will fall into one or more of the following:

- *Operations objectives* - These pertain to the effectiveness and efficiency of the entity's operations, including performance goals and safeguarding resources against loss. When used in conjunction with public reporting, an expanded definition of "safeguarding of resources/assets" can be used: dealing with preventing or detecting and correcting the misappropriation of public funds. The operations objectives need to reflect the particular environment in which the entity functions. As operations objectives are the focal point for directing allocated resources if

they are not clear or not well conceived, resources may be misdirected.

- *Reporting objectives* - These pertain to the reliability of reporting and may involve both financial and non-financial data. Although reporting objectives also relate to information prepared for external parties, the key objective of reliable reporting is to provide management accurate and complete information appropriate for its intended purpose. Without accurate and complete information it is very difficult for management to make good decisions.

- *Compliance objectives* - These pertain to adherence to relevant laws and regulations. The requirements may relate to markets, the environment, employee welfare etc. Some entities will also need to comply with international compliance objectives.

2.2.4 Effective entity risk management provides reasonable assurance that an entity's – operational, reporting and compliance- objectives are being achieved.

2.2.5 Risk appetite, established by management and the board of directors, is a guidepost in setting strategy and assessing the relative importance of objectives. Effectively risk appetite is the level of risk an entity is prepared to accept in providing value (in the form of public services) to stakeholders. Usually any of a number of different strategies can be designed to achieve the desired mission, each having different risks. Management should select the strategy and

associated objectives that best fit in with the risk appetite.

2.2.6 Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. They can be measured through performance targets. Often performance targets are best measured in the same units as the related objectives. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite and will achieve its objectives

2.3 Event Identification

2.3.1 Management identifies potential events that, if they occur, will affect the entity. Events need to be classed as to whether they represent opportunities or whether they might adversely affect the entity's ability to successfully implement strategy and achieve objectives (risks). When identifying events management considers a variety of internal and external factors that could give rise to risks and opportunities, in the context of the full scope of the entity.

2.3.2 An event is an incident or occurrence emanating from internal or external sources that affects implementation of strategy or the achievement of objectives. Events may have a positive or negative impact or both. Events range from the obvious to the obscure and the effects from the inconsequential to the highly significant. However, to avoid overlooking events, event identification is best made apart from the

assessment of the likelihood of the event occurring and its impact.

2.3.3 Management needs to understand the key classes of internal and external factors driving the events. External factors can include but are not limited to those arising from changes in the political environment, the social and technological environment and economic issues affecting either the entity itself or its suppliers. Internal factors stem from choices that management makes about the way it will function. This can include the infrastructure of the entity, how many locations it operates in, the skills and competence of personnel and how business information systems operate.

2.3.4 Event identification techniques look both to the past and to the future. Techniques that focus on past events can consider matters such as annual reports and accounts, payment default histories and internal reports. Techniques that focus on future events can consider factors such as shifting demographics, new market conditions and expected changes in the political environment. Techniques vary widely in their level of sophistication and automation and can be focused on a top down or bottom up view of events.

2.3.5 Events do not often occur in isolation. One event can trigger another and events can occur concurrently. Management should understand how events relate to one another. By assessing the relationships, it may be possible to determine where risk management efforts are best directed.

2.3.6 It may also be useful to group potential events into categories. By aggregating events

horizontally across the entity and vertically within operating units, management can gain an understanding of relationships between events. Grouping events can also give some guidance as to what the most cost effective responses could be. Although each entity will develop its own method of grouping events there are standard tools such as PEST Market Analysis[2] that can serve as a basis.

2.4 Assessing Risks

2.4.1 Assessing risks allows an entity to consider the extent to which potential events have an impact on the achievement of objectives. Management should assess events from two perspectives - impact and likelihood - using a combination of quantitative and qualitative techniques. The positive and negative impacts of events can be assessed either individually or by category for their impact across the entity. Risks should be assessed on both an inherent and a residual basis.

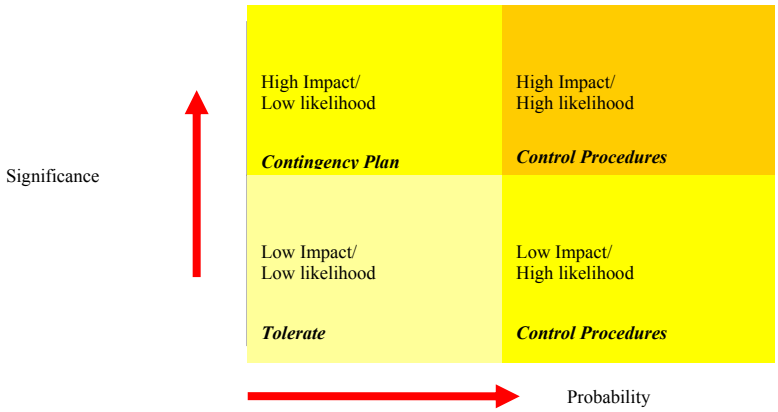
2.4.2 Although the term "risk assessment" sometimes has been used in conjunction with a one-time activity, in the context of Entity risk management, the risk assessment component is a continuous and iterative interplay of actions that take place throughout the entity. The objective of assessing risks is to identify which events are

[2] PEST analysis is a useful tool for understanding and assessing the impact of external factors on the achievement of entity objectives. PEST is an acronym for Political, Economic, Social and Technological factors

important enough and significant enough to be the focus of management attention.

2.4.3 Uncertainty of potential events needs to be evaluated from the perspectives of likelihood and impact. Likelihood represents the possibility that an event will occur in a given period of time, whilst impact represents the scale of the effect that the event will have on the entity's ability to achieve its objectives. The period of time over which management assesses likelihood should be consistent with the time horizon of the related strategy and objectives. The most important risks are those with a high likelihood of occurrence and high impact. Conversely the least important risks are those with a low likelihood of occurrence and low impact. The balance of management focus should be on the high probability, high impact risks (see Figure 2 below). The end result of the process will be to assign each risk a rating for both likelihood and impact. Some entities use a high-low rating, others a "traffic light" system of red, amber and green and others a quantitative measure such as a percentage score.

Figure 2: Simple Risk Assessment and Response Matrix



2.4.4 Risk assessment methodology can be quantitative or qualitative. It can be based on objective or subjective methods. Nor does an entity need to employ common assessment techniques across all business areas. However, management needs to be aware of human bias when assessing risks and needs to ensure that all relevant members of staff have a common understanding of what the rating terminology for assessing risk means. If this is not done it will be difficult for senior management to assess the relevant importance of different risks.

2.4.5 Once risks have been assessed the risk priorities for the entity should emerge. If the risk exposure is unacceptable given the risk appetite of the entity, the risk should be classed as high priority or "key risk". The key risks should be given regular attention at the highest level of the entity. Specific risk priorities will change over time as

the objectives of the entity changes, the risk environment changes and key risks are addressed.

2.4.6 Risk assessment as outlined above pertains to 'inherent risk'. Inherent risk is the risk to an entity in the absence of any actions that management may take to alter the event's likelihood or impact. Residual risk is the risk that remains after considering management's risk response, which is outlined in the next paragraph. The advantage of this method is that it allows entities to identify risks that are taking up management time that could be better spent on other issues (e.g. because the inherent risk has a low probability of occurring).

2.5 Risk Response

2.5.1 Having assessed the relevant risk, management decides how it will respond. Ways to address identified risk include risk transfer, risk treatment, terminating activities and tolerating the risk. In considering its response, management assesses the effect on likelihood and impact, as well as the costs and benefits of each response, with the aim of selecting a response that brings the residual risk within the desired risk tolerance. Management should also identify any opportunities that are available and take an entity wide, portfolio view of risk.

2.5.2 Risk responses fall within the following categories:

- *Sharing/Risk Transfer* - Reducing the risk likelihood or impact by transferring or otherwise sharing a portion of the risk. This

might be done by conventional insurance or by paying a third party to take the risk in another way. This option is particularly useful when mitigating financial risks, risks to assets and for outsourcing activities. However, most risks will not be fully transferable. In particular, it is generally not possible to transfer reputational risk even if the delivery of a service is contracted out.

- *Reduction/Risk Treatment* - By far the greatest number of risks will be addressed in this way. Action is taken to reduce the risk likelihood or impact or both. This typically involves a myriad of everyday business decisions including control procedures discussed in more detail in section 2.6 and in Internal Controls - Integrated Framework.

- *Avoidance/Terminating the Activity* - Exiting the activities giving risk to the risk. Whilst public sector entities are rarely likely to be able to avoid delivering a core programme element, avoidance may be a useful response when considering whether a new method of service delivery is appropriate or considering whether to continue with a specific project.

- *Acceptance/Tolerate* - No action is taken to mitigate risk likelihood or impact. This response suggests that no cost effective response was identified that would reduce the impact and likelihood to an acceptable level or that the inherent risk is already within risk tolerances. Tolerating the risk can of course be supplemented by contingency planning to handle the impacts that will arise if the risk is realised.

2.5.3 The ERM model stresses not just anticipating and managing risks but also, within the same approach, identifying opportunity. In any situation management should look to consider opportunities or events with a positive impact not just consider risk or events with a negative impact. There are two aspects to this: firstly whether or not at the same time as mitigating threats, an opportunity arises to exploit a positive impact; and secondly, considering whether or not circumstances have arisen that, whilst not generating threats, offer positive opportunities.

2.5.4 Management should evaluate the effects of the various methods of addressing the risk, then decide how best to manage the risk, selecting a response or combination of responses designed to bring both risk likelihood and impact within risk tolerances. The selected response need not necessarily result in the least amount of residual risk, but if the response would result in a residual risk that still exceeds risk tolerances, management will need either to reconsider the response or to reconsider risk tolerances.

2.5.5 Evaluating alternative responses to inherent risk requires consideration on additional risks that might result from a response. Here it is helpful for senior management to consider responses from a portfolio perspective as this gives them an overview of the overall risk response profile and enables them to consider whether the nature and types of residual risks remaining are those that fit with the overall mission and risk appetite.

2.5.6 Once management selects the preferred method of addressing the risk it needs to develop an implementation plan. A critical part of every

implementation plan is control activities to ensure that the risk response is carried out effectively.

2.6 Control Activities

2.6.1 Control activities are the policies and procedures that help ensure that management's risk responses are carried out. Control activities occur throughout the organisation, at all levels and in all functions. As the Guidelines for Internal Control Standards for the Public Sector contains detailed information on setting up effective controls, this addendum does not intend to do anything more than put internal controls into the context of Entity risk management.

2.6.2 Entity risk management sees control activities as an important part of the process by which an entity seeks to achieve its business objectives. Control activities are not performed simply for their own sake or because it seems the "right thing to do", but rather serve as mechanisms for managing the achievement of business objectives.

2.6.3 Whilst control activities generally are established to ensure that risk responses are carried out appropriately, in respect to certain objectives, control activities themselves are the risk response. The selection or review of control activities needs to include consideration of their relevance and appropriateness to risk response and the related objectives.

2.6.4 Because each entity has its own set of objectives and implementation approach, there will be differences in risk responses and related control activities. Even if two entities had the same

objectives and made similar decisions on how they should be achieved the resulting control activities would be likely to be different. This is because different management teams will have different risk appetites and risk tolerances.

2.6.5 However, in the context of risk management all control procedures fit into four broad categories:

- **Preventive controls** are designed to limit the possibility of a risk maturing and an undesirable outcome being realised. The greater the impact of the risk on the ability to achieve the entity's objectives, the more important it becomes to implement appropriate preventative controls.

- **Directive controls** are designed to ensure that a particular outcome is achieved. These are particularly important when it is critical that an undesirable event (such as a security breach) is avoided so are often used to support the achievement of compliance objectives.

- **Detective controls** are designed to identify whether undesirable outcomes have occurred "after the event". However, the presence of appropriate detective controls can also mitigate the risk of undesirable outcomes occurring by creating a deterrence effect.

- **Corrective controls** are designed to correct undesirable outcomes that have been realised. They could also act as a contingency to achieve some recovery either of funds or serviceability against loss or damage.

2.7 Information and Communication

2.7.1 There is little difference between the quality requirements of data used to support internal control objectives and the quality requirements of data used to support Entity risk management. As the Guidelines for Internal Control Standards for the Public Sector contains detailed information on information and communication requirements, this addendum does not intend to do anything more than put these requirements into the context of Entity risk management.

Information

2.7.2 Entity risk management specifically requires that an entity capture a greater range of information than is necessary to achieve internal control objectives, for example, the focus on strategic objectives requires more output and outcome information. In addition the use to which this data is put is slightly different. Historical data allows the entity to track actual performance against targets, plans and expectations and can provide early warnings of potential events that require management attention. Present data allows management to take a real-time view of existing risks within a business unit/process and identify variations from expectations. This can allow the entity to determine whether it is operating within risk tolerances.

2.7.3 Pertinent information should be identified, captured and communicated in a form and timeframe that enable staff to carry out their responsibilities. Effective communication also occurs, flowing down, across and up the entity.

All personnel should receive a clear message from senior management that Entity risk management responsibilities must be taken seriously. They need to understand their own role in the Entity risk management process as well as how this relates to the work of others. Personnel must have means of communicating significant information to an appropriate level of management. There also needs to be effective communication with external stakeholders.

2.7.4 Having the right people with the right information, on time and at the right place, is essential to effecting entity risk management.

Communication

2.7.5 Communication is inherent in information systems. As well as providing information to enable appropriate personnel to carry out their duties, communication must take place in a broader sense, disseminating corporate culture, dealing with expectations, covering the responsibilities of individuals and groups, and other relevant matters.

2.7.6 Management provides specific and directed internal communication that addresses behavioural expectations and the responsibilities of personnel. This should include a clear statement of the entity's risk management philosophy and approach. Communication about processes and procedures should align with and underpin the desired culture. Communication should convey:

- The importance and relevance of Entity risk management

- The entity's objectives
- The entity's risk appetite and risk tolerances
- A common language for identifying and assessing risks
- The roles and responsibilities of personnel in effecting and supporting the components of risk management.

2.7.7 There also needs to be methods for employees to communicate risk based information to their line management and across the organisation. Front-line employees who deal with critical operating issues every day are often best placed to recognise problems as they arise. For such information to be reported there must be open channels of communication and a clear-cut willingness to listen. If the corporate culture is one of "shooting the messenger", members of staff will not communicate problems to their superiors and risks may not be identified in a timely fashion.

2.7.8 In most cases normal reporting lines are the appropriate channels of upward communication. However, there are some circumstances where alternative channels of communication (such as some form of whistleblowing hotline) are necessary. Because of its importance, effective Entity risk management requires the existence of an alternative communication channel direct to senior management and available for all staff to use without fear of repercussion.

2.7.9 There needs to be appropriate communication not only within the entity, but with the outside as well. It is important to externally communicate with stakeholders about the way in which the

entity is managing risk to give them assurance that the entity will deliver what is expected and to manage expectations of what can be delivered. This is particularly important in relation to risks that affect the public and where the public depend on their government to manage the risk for them. The seriousness in which communication with external parties is taken and the honesty of such communication also sends important messages throughout the entity and can have a significant impact on organisational culture.

2.8 Monitoring

2.8.1 Entity risk management should be monitored to assess the functioning of its components over time. This can be accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Deficiencies in the Entity risk management system need to be reported to an appropriate level of management, with serious matters reported to senior management or the board in order for the entity to improve its processes.

2.8.2 The objectives of an entity may change over time. The portfolio of risks faced and their relative importance is also likely to change over time. Risk responses that were once effective may become irrelevant or impossible to implement, and control activities may become less effective or lapse altogether. Management needs to constantly monitor the effectiveness of their risk management system in order to determine whether it is still appropriate and effective.

2.8.3 Evaluations of the effectiveness of risk management will vary in scope and frequency, depending on the significance of groups of risks and the importance of risk responses and related controls in managing those risks. When management makes the decision to undertake a comprehensive evaluation of the risk management framework, attention should be directed to addressing every aspect of the process including strategy setting. However, regular management activities such as updating risk registers and organisational or functional "health checks", also form part of monitoring the risk management process.

Bibliography

Australian Standard® for risk management (Standards Australia, 2004)

Entity Risk Management - Integrated Framework (COSO, 2004)

Integrated Risk Management Framework (Treasury Board of Canada Secretariat, 2001)

Internal Control - Integrated Framework (COSO, 1992)

Risk Management Standard (ARMIC, IRM & ALARM, 2002)

The Orange Book: Management of Risk - Principles and Concepts (HM Treasury, 2004)