RISK MANAGEMENT GUIDELINE FOR SAIs

2010

FOREWORD

The AFROSAI-E's mission is to enhance the institutional capacity of SAIs. Risk management was identified as one of the pertinent issues that heads of SAI had to address in the execution of their SAI mandates during the IDI/AFROSAI-E Management Development Programme (MDP): "Leading an SAI" Workshop for Heads of SAIs and their Deputies. The AFROSAI-E was mandated to develop the necessary guidance materials to assist SAIs to manage the associated risks that they are exposed to in their different operating environments.

There is an increasing challenge for Supreme Audit Institutions (SAIs) to continue improve in order to better serve public interests. Consequently, putting in place good governance procedures which include risk management is a must for every SAI. This is expected to result in SAIs becoming more proactive, result oriented, add greater value to better serve public interests and improvement in the management of the SAIs.

This guideline is based on the INTOSAI's GOV 9130 for Internal Control standards for the Public sector- 'Further Information in Entity Risk Management" which is based on the Committee on Sponsoring Organisations (COSO) of the Treadway Commission's integrated framework for internal control.

The purpose of this guideline is to provide practical guidance on how the SAI's management can develop risk management frameworks/ policies, design and implement risk management plans or strategies across their SAIs. If applied, this guideline will help SAIs to effectively achieve their mandates.

The guideline was developed by a team consisting of Gorden Kandoro, Josephine Mukomba, Louis Heunis (AFROSAI-E Secretariat) and Khemraj Reetun (Mauritius). The team would like to acknowledge the SAIs of South Africa and Eritrea for sharing their experiences.

This guideline is a living document and will be updated in line with new experiences.

Pretoria, November 2010.

Wessel Pretorius

Executive Officer

AFROSAI-E Secretariat

CONTENTS

ABOUT THIS GUIDELINE

Why a Guideline?

The aim of this guideline is to assist SAIs develop and implement a practical approach to implement the techniques and procedures of risk management.

Entity risk management as it relates to an SAI is a decision making tool that helps to systematically identify risks and determine the best courses of action for any given situation.

Objectives of this Guideline

The objective of this guideline is to provide guidance on how SAIs management can develop risk management frameworks in their SAIs. It provides a step by step approach to entity risk management.

The guideline is expected to:

- Provide SAIs with key principles and concepts, a common language and clear direction and guidance regarding the management of entity risks;
- Assist SAIs to plan and manage risks in their operating environment;
- Provide a risk management framework for those SAIs embarking on entity risk management for the first time;
- Contribute towards the implementation of risk management plans and or strategies; and
- Set the scene for continual improvement in the manner a SAI delivers its services.

Who can use this Guideline?

SAIs can use this guideline during the risk management process which includes the setting up of a conducive internal risk management environment, goals and objectives setting, risk identification, assessment and response, risk mitigation activities, information and communication with stakeholders and monitoring and reviewing of the risk management strategies. The guideline should be used in conjunction with the IDI/AFROSAI-E Strategic Planning Handbook as well as other AFROSAI-E guidance materials. Before applying the guideline, it is important that users understand their SAI's strategic and annual planning processes as well as the application of the various policy documents governing the organisation of the SAI.

Heads of SAIs or Boards, senior managers, operational managers, staff and other specially assigned members are encouraged to use this guideline to ensure that risk management is embedded in the planning processes as well as in the day to day operations of the SAIs.

How to use this Guideline?

The guideline is based on the INTOSAI GOV 9130, "Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management," as set out in the Integrated Entity Risk Management (ERM) Framework of the Committee on Sponsoring Organisations (COSO) of the Treadway Commission. The guideline applies the COSO–ERM Integrated Framework definitions of risk and risk management and surrounding risk issues and concepts with the objective of ensuring that the resultant SAI risk management framework is properly aligned to the SAI strategic goals and objectives. The guideline outlines the roles and responsibilities of heads of SAIs or Boards and managers who are involved in the management of risks. Consequently, this guideline encourages SAIs to develop and establish risk management frameworks based on the boundaries set by their risk management philosophies, risk appetite and risk culture.

This guideline is divided into eleven chapters. The first three chapters outline the concept of risk, risk management and related terms based on the COSO- ERM Integrated Framework. The last eight chapters address the issue of how the eight interrelated components of ERM as set out in the COSO model can be applied by SAIs in managing risks associated with their individual operating environment.

Chapter 1

GOVERNANCE FRAMEWORK OF AN SAI

1.0 Introduction

Contemporary organizational management philosophies require the management of risk across the entir organization. In order to ensure the achievement of organizational objectives, there is need to effectivel and holistically integrate risk management with corporate governance processes[1]. In an SAI, the head o SAI or Board is responsible for the corporate governance oversight while the SAI management is responsible for risk management processes. Good governance in an SAI on its own does not guarantee success unless the associated risks are effectively identified, analysed and managed.

1.1 Risk Governance Framework of an SAI

Good corporate governance is a fundamental requirement for any successful organization. The INTOS Guidance for good governance (GOV) - (ISSAI 9000 series[2]) encourages SAIs to establish internal control structures and systems that include the management of risks. These GOVs are aligned to the Committee on Sponsoring Organisations of the Treadway Commission's (COSO) [3]-framework for internal control, which is internationally recognised.

INTOSAI also expects SAIs to demonstrate their value and benefits to society by establishing among other things good governance structures to enable their leadership to make decisions and manage risks towards achievement of their goals and objectives. The guiding principle of the above stated requireme of ensuring good governance arrangements within a SAI include:

- *"Organizational risk being assessed on a regular basis and backed up with appropriately implemented and regularly monitored risk management initiatives.*
- *An appropriately objective internal audit function being an integral part of the SAIs' operation risk management strategy."* [4]

[1] In an SAI governance describes the overall management approach through which heads of SAIs or Boards exercise oversight direct and control the entire organization, using a combination of management information and hierarchical management contr structures to enable appropriate decision making, and provide the control mechanisms that ensure that SAI directives and instructions are carried out effectively.

[2] INTOSAI GOVs: - 9100: *Guidelines for internal control standards in the public sector;* 9110: *Guidance for reporting on the effectiveness of internal controls;* 9120: *Internal control – providing a foundation for accountability in government;* 9130: *Guidelines for internal control standards in the public sector-further information on entity risk management;* 9140: *Internal a independence in the public sector* and 9150: *Coordination and cooperation between SAIs and internal auditors in the public sector*

[3] The Committee of Sponsoring Organisations (COSO) of the Treadway Commission is a voluntary private-sector organizatio established in the United States of America in 1985, dedicated to providing guidance on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. COSO was formed tc sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission). The Commission was sponsored and funded by five main professional accounting associations and institutes: the *American Institute of Certified Pub Accountants* (AICPA), *American Accounting Association* (AAA), *Financial Executives International* (FEI), *Institute of Intern Auditors* (IIA) and the *Institute of Management Accountants* (IMA). These five organizations formed what is now called the Committee of Sponsoring Organizations of the Treadway Commission.

[4] The XX International Congress of Supreme Audit Institutions (ICOSAI) Theme Paper 1 : The 2010 XX INCOSAI Theme 1 Principle Paper: Value and Benefits of SAIs outlines the need for "Good governance arrangements within the SAIs" as a fundamental requirement.

Furthermore, SAIs are expected to uphold the principle of "leading by example". For instance, ISSAI 1315 requires SAIs to assess the risk management process of an audited entity. It follows that SAIs should also adhere to the same, appropriate rules and requirements (at principle level) that SAIs expect from auditees.

The concept of risk governance stated in the above requirement does not only include "risk management' or "risk analysis' but also addresses how risk related decision-making is coordinated in the execution of the SAI's goals, objectives and activities. According to the INTOSAI Govs every member SAI is encouraged to establish its own risk governance framework that ensures the achievement of its strategic goals and objectives.

1.2 SAI Responsibilities in setting up a Risk Management Framework

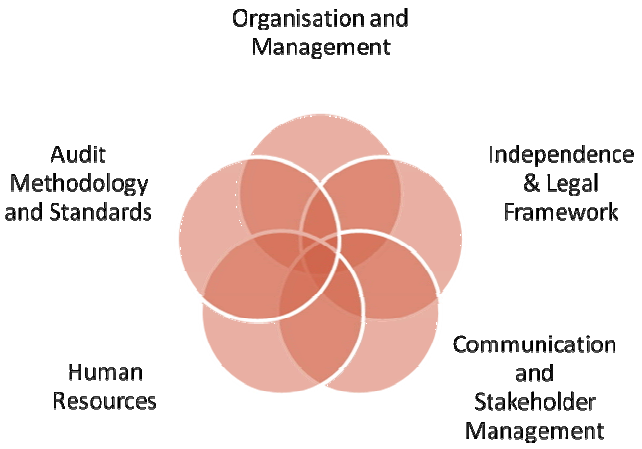
The head of the SAI or Board should be involved in the entity's risk management process by providing direction, authority, and oversight to management. In order to ensure an effective risk governance framework the head of the SAI or Board should:

- Contribute expertise, judgment, and professional skepticism to the strategic planning and operational planning processes;
- Define and communicate risk tolerance thresholds to senior management to guide management's decisions;
- Assign authority to senior management to manage risks within the specified tolerance levels;
- Oversee the implementation of the SAI's risk management process, and monitor the process to ensure that it operates effectively; and
- Ensure that management's mix of performance indicators associated with key risks is aligned wit the SAI's strategy and linked to the creation of stakeholder value. The head of SAI or Board should hold senior management accountable for keeping the SAI appraised of significant risks, taking appropriate actions to manage these risks, and reporting risk management performance results.

1.3 AFROSAI-E's Institutional Capacity Building Framework (ICBF)

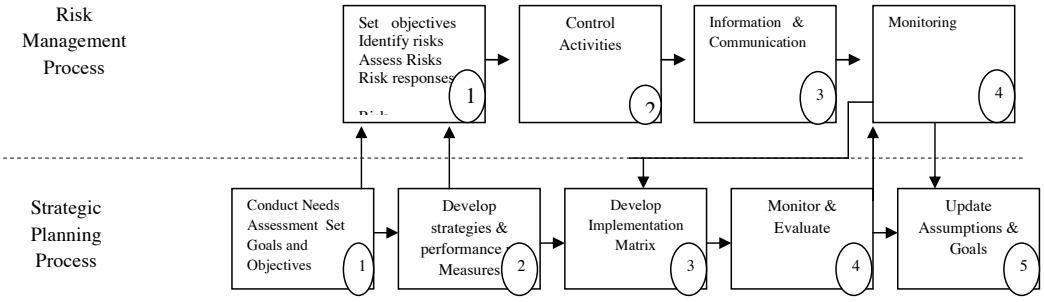
The AFROSAI-E Institutional Capacity Building Framework (ICBF) provides comprehensive set c provisions defined in five domains, towards which all SAIs should work (illustrated in Figure 1 below). I each of the above five domains function effectively and delivers the desired results, it can be reasonabl be expected that the SAI as a whole will deliver high quality products and services. The ICBF c AFROSAI-E is the framework leading the development of SAIs in the region and as such it should als lead the risk management process of an SAI. The domain of, "Organisation and Management," include the leadership and direction of the SAI, strategic and operational planning, the code of conduct, qualit assurance, internal controls, infrastructure and technology. One of the key elements under this domain i the requirement for an SAI to develop and implement an effective internal control system. INTOSA GOV 9100 describes internal controls as constituted by five components namely; control environmen risk assessment, control activities, information and communication and monitoring.

Figure 1: The five Domains of the AFROSAI-E Institutional Strengthening Framework



It should be noted that risk management is not an isolated process within an SAI separate from strategic and operational planning. Risk management should be seen as a normal part of the SAI's strategic and operational planning process within a SAI. The diagram below shows the integration of risk management and strategic planning and control processes to illustrate that entity risk management is not an isolated process.

Figure 2 – An integrated risk management and strategic planning and control process



The integration at the different phases will be further elaborated in the ensuring chapters.

Chapter 2

RISK MANAGEMENT CONCEPTS AND RELATED TERMS

2.0 Introduction

Risk management is both a strategic and operational function that must be performed by management. This chapter addresses the concept of risk, risk management, definitions and related terms.

2.1 What is risk?

The Institute of Internal Auditors defines risk as *"….the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood."* Similarly, the Committee of Sponsoring Organisations (COSO) of the Treadway Commission defines risk as *"…the possibility that an event can adversely affect the achievement of an objective."* In other words risk involves the deviation of one or more results or future events from their expected results.

2.2 What is Risk Management?

Risk management is a process that serves as a component of corporate governance as it indirectly affects a SAI's achievement of goals and objectives. Managers control risks when they modify the way they do things to make their chances of success as great as possible while making their chances of failure, as small as possible. Risk management is premised on the philosophy that it is irresponsible and wasteful to wait for an adverse event to happen and then find ways to deal with the event to prevent it happening again.

Risk management is a function aimed at protecting the organization, its human capital, production processes/systems, products and other assets against the physical and financial consequences of event risk. In other words SAI managers have a responsibility of planning, directing and coordinating the risk control and risk financing activities of the SAI. SAI risk management is both a strategic and operational function.

SAI managers should take the necessary steps to identify, categorize and rank the risks it is exposed to according to their likely impact with the aim of taking a decision on how best the risks can be managed. This should include taking steps to identify the various threats affecting an operation and determining the magnitude of the potential loss associated with those threats using qualitative or quantitative methodology. It involves identification, examination, prioritization and mitigation of various potential and real threats or hazards that an SAI is facing.

2.3 Benefits of Risk Management

There are a number of benefits for a SAI to have a risk management framework in place, including the following:

- Improvement of service delivery by the SAI
- Protecting the reputation, credibility and status of the SAI
- More effective strategic planning within the SAI
- Better workflows and auditee evaluation and engagement process
- Ensures the protection of asset, finances and SAI operations.

2.4 Relation to Other SAI Processes and Documents

The overall vision, mission and strategic objectives of the SAI should form the basis for the development of risk management process. The risk management process should be integrated into the SAI's strategic and operational planning, implementation, monitoring and evaluation activities. As such risk management should be made an integral part of all other SAI processes by making it;

- part of every process within the SAI and
- a responsibility of everyone within the SAI.

Prior to finalizing its strategy, management must ensure that the SAI strategy is within its overall risk appetite unless the strategy requires the overhauling of the existing risk management policy. It is for this reason that the development of risk management in an SAI should grow in harmony with the development of the SAI. Thus risk management should be a central part of the SAI's strategic management process.

Chapter 3

The Entity Risk management Framework – An Overview

3.0 Introduction

In order to be effective risk management should function within a risk management framework. Such a framework should provide the foundations and organizational arrangements that will embed it throughout the SAI at all levels. There are several risk management frameworks[5] and approaches that an SAI can adopt or adapt to address the risk governance challenges in its operating environment. This guideline uses the COSO-Entity Risk Management (ERM) -2004 framework because it is the one that the INTOSAI GOV (ISSAI 9130) encourages SAIs to use.

This chapter summarises the COSO-ERM Integrated Framework, the concept of entity risk management, the eight components of ERM, objectives and levels of risks that a SAI is exposed to in its operating environment. It also introduces the COSO – ERM model as the framework for implementing risk management in an SAI.

3.1 The COSO Entity Risk Management Framework

COSO's Entity Risk management: Integrated Framework states that:

> *"… risk management is a process effected by the 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 within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"*

ERM focuses on three primary risk drivers: 1) risk identification and understanding; 2) risk acceptance and tolerance; and 3) risk management and mitigation surrounding all organizational data and functions. ERM is more than just a compliance initiative. It involves a process, facilitated by an organization's management and support personnel which is applied across the entire entity and is designed to identify and manage potential risks that may have an adverse effect on the entity's ability to achieve its strategic objectives.

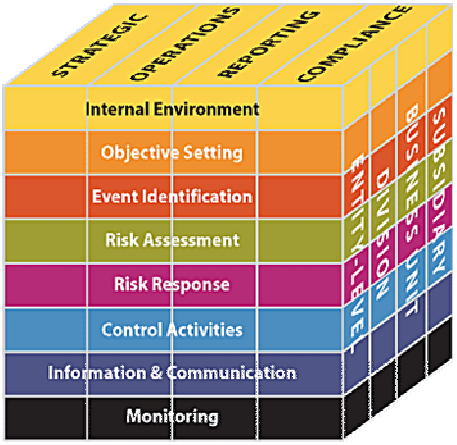
The goal of the COSO-ERM framework is to provide SAIs with key principles and concepts, a common language and clear direction and guidance regarding the management of entity risks. It is a systematic approach to managing risk throughout the organisation and provides assurance about the achievement of its objectives. ERM empowers SAIs to identify the steps they can take and the resources they should

[5] Some of the risk management frameworks include; the COSO - Enterprise Risk Management -2004; the International Standards Organisation (ISO) 31000 "Risk Management – principles and Guidelines)-2009;" the Australian/ New Zealand (AS/NZS 4360 Risk Management Standard; GRC (Governance, Risk and Compliance) Capability Model – 2010 and others.

allocate to overcome or mitigate risks, and to provide reasonable assurance about the achievability of their objectives.

The COSO-ERM framework comprises eight interrelated components which are derived from the manner management drives a business and are integrated with the organisation's management process. The framework satisfies the internal control needs of an SAI and further allows for the integration of risk management process into the day to day operations of the SAI. Figure 3 below shows the depiction of the components and how they are related to the entity objectives and the levels at which risks can occur within an SAI:

Figure 3: COSO's ERM requires an entity to take a *portfolio view* of risk.



The COSO ERM model views entity objectives in the context of four categories which are namely, strategic, operations, reporting and compliance. There is a direct relationship between entity objectives and entity risk management components. The components represent what is needed to achieve the entity objectives. The relationship is depicted in a three-dimensional matrix (refer to figure 1 above) popularly known as the COSO cube. The vertical columns represent the four objectives categories and the eight components are the horizontal rows and the third dimension is representing the entity's units. This depiction provides SAI managers with the ability to focus on the whole entity's risk management by objectives category, component, entity unit or any subset thereof. The approach of entity risk management provides reasonable assurance that an entity's –strategic, operational, reporting and compliance- objectives are being achieved in an effective manner. The components themselves are also criteria for effective entity risk management.

3.2 Entity objectives are classified in four main categories

The COSO – ERM framework is focused on achieving an entity's objectives, classified in four categories:

1. ***Strategic objectives*** **-** High level goals, aligned with and supporting the entity's mission.

2. ***Operational objectives*** **–** Executing orderly, ethical, economical, efficient and effective operations; and safeguarding resources against loss, misuse and damage;

3. ***Reporting objectives –*** These objectives involves issues of reliability of reports including fulfilling accountability obligations;

4. ***Compliance objectives –*** Compliance with applicable laws and regulations.

An SAI will create stakeholder value if it manages risks in the above four categories within its risk appetite.

3.3 Components of the COSO's ERM Framework

Risk management should be an ongoing process at every level of the SAI. From a COSO ERM Framework perspective, risk management consists of eight interrelated components. The components are derived from the way management runs the entity and are integrated with the entity's strategic and operational management processes. The components are as follows:

1. **Internal environment** – It is the foundation of all the other components. It encompasses "the tone of the SAI" at the top and sets the basis of how risk and control are perceived and addressed by an entity's people, including risk management philosophy, and risk appetite, integrity and ethical values and the environment in which they operate .
2. **Objective setting** – Objectives must be set before management identify risks that can affect their achievement. A precondition to risk assessment is establishment of objectives, linked at different levels to the SAI's mission and internally consistent with its risk appetite**.**
3. **Event identification** – Events that might have an impact on the entity's achievement of its objectives must be identified. Event identification involves identifying potential events from internal or external sources affecting achievement of the SAI's objectives. It also involves distinguishing between risks and opportunities whereby the opportunities are channeled back to the SAI's strategy or objective setting processes.
4. **Risk assessment** – Risks are analysed, considering likelihood and impact, as a basis for establishing the approaches needed to manage them. Risks are assessed on an inherent and residual basis. Risk assessment also involves analyzing and evaluating the identified risks on a continuing basis and identifying high and low risks and their associated impact on the business of the SAI.
5. **Risk Response** – It involves the identification and evaluation of possible responses to risks which may include transferring, reducing, avoiding or accepting risks. Management should then select a set of actions or activities to align risks with the SAI's risk tolerance levels and risk appetite.
6. **Control Activities** – Under this component policies and procedures are designed and implemented to help ensure that the risk responses are effectively carried out.
7. **Information and Communications** – Relevant information is identified, captured and communicated in a form and timeframe that enable the various players to carry out their responsibilities. Information is needed at all levels of the SAI for identifying, assessing and responding to risks. It means communication and consultations with all the levels and different parts of the SAI as well as outside parties should be done so as to ensure that all are well informed.
8. **Monitoring** – The entirety of ERM should be monitored and modifications made as when necessary. This involves the monitoring and reviewing of the risk management strategies that have been developed and implemented. It should be based on current changes to the operating business environment.

In the following chapters we shall be dealing with the detailed parts and concepts constituting the eight components summarized above, starting with the internal environment.

Chapter 4

INTERNAL ENVIRONMENT

4.0 Introduction

This chapter deals with the SAI's internal environment as the foundation of risk management. It focuses on the enabling environment for risk management in an SAI. It explains the different concepts that form the different interrelated layers that constitute the internal environment. The concept of risk philosophy, risk appetite, risk culture and other related terms are explained including organization of the different authority levels.

4.1 Creating an Enabling Environment for the Management of Risk

The head of SAI or Board is responsible for ensuring that the SAI's internal environment supports the effective functioning of risk management. In other words the institutional environment is the foundation of risk management through providing the culture, discipline and structure that influences how SAI activities are planned and executed and how risks are identified, assessed and managed.

In order to create an enabling environment for the management of risks, the head of SAI should ensure that the SAI:

- Operates within its constitutional mandate;
- Adopts a value system founded on SAI ethos
- Possesses the inherent staff competencies required to execute its mandate
- Adopts management practices that embrace the concept of delegation of authority, personal responsibility, transparency and accountability and performance management;
- Establishes an appropriate organizational structure supported by basic financial and management systems geared by risk management and internal controls.

The head of SAI or Board is expected to establish the SAI's risk management philosophy, its risk tolerance levels (appetite), inculcate a risk culture and integrated risk management in the SAI activities. The internal environment consists of eight different layers that should all be present and functioning which are namely;

- Risk Management philosophy
- Risk appetite
- Risk culture
- Integrity and values
- Commitment to competence
- Organisational structure, authority and responsibility

- Human resources capacity, policies and procedures
- Tools, technology and related costs

Risk management philosophy

Risk management philosophy[6] is the set of preferences, value judgments and attitudes characterizing how the SAI handles everything it does, from developing and implementing strategy to day-to-day activities. This philosophy reflects the SAI's values, influencing its culture and operating style, and affects how well fiscal programs can be implemented, maintained, and enforce control.

Risk appetite and tolerance

Risk appetite is the residual risk the SAI is willing to accept or tolerate in seeking to achieve its objectives. The head of SAI or Board should determine the levels of risk tolerance by setting rules for risk taking in respect of all types of risks. These rules of risk tolerance limits should be reviewed during periods of increased uncertainty or adverse changes in the environment. In setting the risk tolerance levels, management should consider risk factors in both the external and internal environments. The levels could be measured quantitatively, qualitatively, or both, and should be specific to each of the relevant SAI activities.

Risk appetite and tolerance involves management implementing specific limits or tolerance levels that are aligned with those overall limits set by the head of SAI or Board at departmental or functional, activity and operational risk levels. The risk appetite limits should be communicated in the SAI's Risk Management Policy and or Risk management Plan/Strategy. Where, management at departmental or functional, unit or activity level deviate materially from the risk appetite set by the head of SAI or Board this should be reported directly together with the reasons warranting the deviation.

Risk Culture

Risk culture is the appearance and attitude of management regarding Entity Risk Management that is communicated to the SAI personnel. It can also be the set of shared attitudes, norms, values and practices that characterize how a head of SAI or Board considers risk in its day to day activities. The SAI's Risk Management Policy should define and state its risk culture based on its strategic goals and objectives.

Integrity and Values

The way strategy and objectives are formulated, implemented and achieved is based on the preferences, value judgments and management styles of the different SAIs. As such management 's integrity and commitment to ethical values influence these preferences and value judgments which are then translated into standards of behavior. The head of SAI or Board significantly influences the SAI's control environment elements.

The integrity of management is a prerequisite for ethical behavior in all aspects of the SAI's activities. It is expected that management lead by example as regards expected ethical behaviors and attitudes. A Code

[6] The risk philosophy of management is usually stated in policy statements, oral and written communications, meetings, decision-making by the head of SAI or Board and other channels of communication.

of Conduct is important to the foundation of an effective ethics programme in an SAI. It addresses a variety of issues, such as integrity and ethics, confidentiality, conflicts of interest, illegal or otherwise improper payments, corruption and other arrangements. The head of SAI or Board should ensure all SAI employees comply with the SAI's Code of Conduct. There should be a mechanism in place to encourage employees to report all suspected fraudulent behavior by other employees, corruption and theft and punitive disciplinary measures against employees who fail to report violations.

Commitment to Competency

Competence reflects the knowledge and skills needed to perform assigned tasks. The head of SAI or Board should ensure that the competency levels for each audit assignment is specified and translated to requisite knowledge and skills. However, a trade-off exists between competence and costs. For example, a trade-off can be made between the extent of supervision and the requisite competence level of the individual carrying a given audit task. However, it should be noted that management style could also determine the way the SAI staff members are managed and what kinds of risks should be accepted.

Human Resources Capacity, Policies and Procedures

Adequate human resources capacity, represented by appropriate number of people with the right skills mix and qualifications is fundamental to implementing an effective risk management strategy. Internal processes should be established to sensitise all employees of the relevance of risk management to the achievement of their performance goals. The SAI should have in place human resources policies, rules and regulations for guiding the hiring, orientation, training, evaluating, counseling, promotion, compensation and disciplining of SAI staff. It is the responsibility of the SAI to ensure that all its employees are well equipped to handle new challenges as issues and risks throughout the SAI change and become more complex.

Depending on the operational capacity, size and structure of the SAI a Risk Committee or Risk Coordination Officer could be responsible for directing and coordinating the entity-wide risk exposure of the SAI including the strategic risks, business risks, the operational risks, reputational risk and maybe even the legal and regulatory compliance risks. Individual managers should be assigned to manage risks in their areas of responsibilities and report to the committee or other instructed lines of reporting. Their job responsibility should be about three things: identification of risk; measurement and recommendation of risk tolerances or appetites for the SAI; and the management of risk, how the SAI lay off or transfer unwanted risk given the appetite for risk at the strategic and operational level of the SAI.

The SAI should ensure that everyone involved in risk management is provided with training and adequate support in order to carry out their personal responsibilities in an effective and efficient manner.

Organisational Structure

An SAI's organisational structure provides the framework to plan execute, control and monitor its activities. A relevant organisational structure includes defining key areas of authority and responsibility and establishing appropriate lines of reporting. The appropriateness of a SAI structure depends in part on its strategy, size and range of its audit mandate.

For effective risk management the head of SAI or Board should delegate roles and responsibilities in a manner that ensures effective coordination and synergy of risk management activities. This requires

structuring and coordinating the work of departments, divisions, business units and teams in a way that provides a complete perspective of the SAI's risk exposures and opportunities. The type of risk governance structure put in place should be driven by the SAI's mandate and operating realities of capacity constraints. The risk function may range from a part-time risk manager or coordinator or committee to a full-scale risk management department or division reporting to the head of SAI or Risk Management Committee.

Tools, Technology and Related Costs

The SAI should make appropriate choices regarding the use of automated data capturing tools, organizing, storing and interrogating data as well as communicating and tracking information for decision making purposes. Appropriate tools and technology can facilitate considerable efficiencies by simplifying complex audit and support processes and accelerating otherwise time consuming tasks in the risk management process. However, it should be noted that technology does not substitute the need of human intervention and intellect.

Decisions for investment in risk management and control technology should be considered on the basis of cost versus benefit. The overall budget for risk governance is the responsibility of the head of SAI or Board but can be delegated to the Risk Committee or Risk Coordination Officer or other teams like the strategic planning and implementation team of an SAI. Implementing and improving risk management and controls is the responsibility of the respective risk owners.

Once the above different layers of responsibility assignment are in place the SAI should then produce documents that would guide the SAI in managing the different risks that it is exposed to. The risk management policy and risk plan/strategy are two key documents which can be used by an SAI to manage and communicate its risk management strategy.

4.2 Risk Management Policy

The risk management policy expresses an SAI's commitment to risk management and clarifies its general direction or intention. The risk management policy should:

- State the approach or framework followed, (for instance, COSO, ISO, IRMSA, ERM Code of Practice, IRM (UK).
- indicate how risk management will support the SAI's strategy
- Spell the SAI's definitions of risk and risk management, the risk approach, philosophy and appetite as they apply within the SAI's context;
- Identify and define the various responsibilities for risk management within the SAI.
- Establish the SAI's risk management architecture and reporting lines
- Incorporate a statement committing the SAI to implement and maintain an effective, efficient and transparent system of risk management
- Include the risk management guidelines;

Contents of a Risk Management Policy

A Risk Management Policy should include the following sections:

Introduction

- Vision, mission, values and strategic goals and objectives
- Risk Governance - Risk management and internal control objectives
- Main risks that the SAI is exposed to
- Risk Framework of the SAI

The internal Environment

- Statement on the definition of risk, risk management, risk philosophy, appetite and tolerance levels
- Risk management organisation and allocation of roles and responsibilities including Management approval framework
- Risk management training topics and priorities
- Criteria for allocation of resources based on the levels of risk exposure

Risk Management Process

- Objective setting – strategic goals and objectives
- Event Identification –details of procedures for risk recognition
- Risk assessment – details of procedures for risk ranking
- Risk response – Risk mitigation requirements
- Control Activities – control mechanisms
- Information and Communication – criteria for gathering and recording information and lines of communication
- Monitoring –criteria for monitoring and benchmarking of risks

Some SAIs can choose to have separate documents for the risk management framework and strategy. What is important is to ensure that the key information is included in the available documents. The risk management policy should be widely distributed throughout the SAI. Refer to **Appendix 1** for a generic Risk Management Policy for an SAI.

4.3 The Risk Management Plan

An SAI's risk management plan describes how it intends to manage risk. It describes the management components, the approach, and the resources that will be used to manage risk within a given period which is usually a year. Typical management components include procedures, practices, responsibilities, and activities (including their sequence and timing. The risk management plan should be tailored to the specific circumstances of the SAI based on its risk management policy. (Please refer to Annexure C for an example of a risk Plan). The risk management plan should include:

- the SAI's risk management structure as stated in the risk policy;
- A plan of action to improve the SAI's risk management maturity which can be in the form of a risk register; The risk register is discussed in the next chapters.
- the standards and methodology adopted – this refers to the measureable indicators such as tolerances, intervals, frequencies, frequency rates, etc;
- details of the assurance and review of the risk management process; and
- reference to integration through, for instance, training and awareness programmes.
- Organizational structure, human resources capacity and tools, technology and costs of implementing and maintaining the SAI risk management plan.

The management should review the SAI's annual risk management plan regularly, at least once a year. The head of SAI or Board should ensure that the implementation of the risk management plan is monitored continually.

4.4 Oversight by the Head of SAI or Board

The head of SAI or Board should be responsible for the governance of risk. In particular he/she should exercise leadership to prevent risk management from becoming a series of activities that are detached from the realities of the SAI's business.

Where the head of SAI or Board has delegated its responsibility for risk management to a Risk Management Committee or Risk Management Coordinator, or the SAI's Strategic Planning and Implementation team the terms of reference should reflect this responsibility and should be approved by the head of SAI or Board.

Assignment of authority and responsibility

The risk committee or team or officer assigned the risk coordination responsibility should draft or review the risk management policy and plan, and should monitor the whole risk management process. Members of the risk committee or team, taken as a whole, should comprise people with adequate risk management skills and experience to equip the committee or team to perform its functions. To supplement its risk management skills and experience, the risk committee or team may invite independent risk management experts to attend its meetings.

If a committee or team is set up it should have a minimum of three members and convene at least once a year.

Please refer to Appendix 1 *Generic Risk Management Policy for a SAI* for detailed roles and responsibilities.

CHAPTER 5

OBJECTIVES SETTING

5.0 Introduction

It is important to note that there is no separate objective setting process for risk management but it is intertwined with the strategic and annual planning processes as shown in previous chapters. The setting of objectives is an essential step in the risk management process. Objectives must be established before management can identify and assess risks to their achievement and take the necessary actions to mitigate those risks.

5.1 Important Considerations

The components of the internal environment outlined in Chapter 4 which include risk management philosophy, culture, integrity, values and organisational structure will affect the setting of objectives in a SAI. In particular, risk appetite will be a key consideration in objective setting and strategy selection. If a SAI is setting very ambitious goals, then it should have an appetite for a commensurate level of risk. An example is when a SAI sets out to introduce new methodology and increase audit coverage at the same time. Conversely if an SAI is very risk averse i.e. has a low appetite for risks then one would expect that SAI to set more conservative goals.

5.2 Categories of Objectives

INTOSAI GOV 9130 sub – divides objectives into four categories which are; strategic, operational, reporting and compliance. In order to align with the *AFROSAI-E/IDI Strategic Planning handbook and Annual Planning for SAIs,* in this guideline the objectives will only be described in two categories which are strategic and operational objectives.

5.3 Strategic Objectives

Strategic objectives require multiple years to be achieved and so have a time horizon of three to five years. Strategic objectives are high level goals. It is important that strategic objectives are aligned with the SAI's mission. They reflect management's choice as to how the SAI will attempt to create value for its stakeholders. In the Strategic Planning Handbook these are referred to as goals.

As stated in the introduction, the strategic objectives are set during the strategic planning process. Some of the objectives can be reviewed during the annual planning process. Since SAIs have in most cases similar mandates, their objectives would broadly be the same. A look at examples of objectives of some AFROSAI-E SAIs would show that mostly the same issues are being addressed. Below is an extraction from the Strategic Planning Handbook which shows the typical development goals for SAIs in the AFROSAI-E Region:

- To make the SAI independent and accountable
- To provide timely and high quality audit services
- To have an adequate and competent workforce
- To establish a modern and effective organisation and management system
- To enhance the image and impact of the SAI.

Please refer to the Strategic planning Handbook for more details on how to set high level goals and objectives.

5.4 Annual Operational Objectives

In order to achieve strategic objectives, the organisation needs to set annual operational objectives that coincide with a calendar year, a fiscal year, or the organisation's operating cycle. Operational objectives also need to be further divided into objectives for business units, departments, functional areas, teams, and individuals. Please refer to the Operational Planning exposure draft in relation to setting annual objectives. Examples of annual objectives are as follows:

- To improve staff establishment by 10%
- To implement a management information system.

5.5 Conclusion

Objective setting is key to risk management. This sets out the foundation for the next process which is risk identification.

CHAPTER 6

RISKS IDENTIFICATION

6.0 Introduction

The objective of the chapter on risks identification is to enable users to have a holistic approach to identify risks in SAIs. Once objectives have been set, an SAI should identify events that might have an impact on the achievements of these objectives.

6.1 What is Risk Identification

Risk identification involves identifying potential events, occurring internally or externally, that could affect achievement of objectives. It addresses how internal and external factors combine and interact to influence the risk profile.

Risk identification should not limit itself to a fixed list of risk categories. Risk identification is most effective when it is directed towards the SAI's objectives. It is important to ensure that an all-embracing approach which includes both strategic and operational objectives is adopted.

Events that may have a negative impact represent risks and can hinder the SAI's ability to achieve its objectives. Risk identification produces the required information for the ensuing risk management processes, It is therefore critical that the process is accurate, thorough and complete.

6.2 Who should be involved

Risk identification should not rely solely on the perceptions of a select group of managers. Top and senior management would normally be involved in the identification of strategic risks while senior and operational managers will be involved with operational risks. Other participants in risk identification activities can include, where appropriate: team members, risk management team, the SAI's quality assurance function, subject matter experts, and stakeholders

The strategic and operational planning teams and participants would ideally be involved since the processes are linked.

6.3 Process of Risk Identification

Risk identification could be done as a separate process after completing the strategic planning especially when the SAI is embarking on the process for the first time. However for future risk identification processes, it is recommended that there is a linkage with the strategic planning process. During strategic planning, the risk identification process will already start as the SAI conducts the needs assessment or the situational analysis. However since the process is based on established objectives, the process can only be finalized after identifying the goals/objectives of the SAI.

Some external factors to be considered for potential risks include:

- Political – for SAIs this could affect the independence, mandates or reporting on findings
- Economic: whether international or national economic issues – have a bearing on funding and achievement of goals
- Social: - affects organisational cultures, structures, productivity etc
- Technological: - affect infrastructure, information systems

Internal factors reflect management choices and include:

- The overall management framework
- Governance and accountability frameworks
- Values and ethics
- Infrastructure
- Policies, processes and procedures
- Human resources capacity
- Technology

6.4 Methods of identifying risks

The possible methods include the following:

- Interview /focus group discussions- for example gather together top and senior management to brainstorm on possible risks to achievement of objectives on different levels.
- Survey, questionnaire
- SWOT analysis
- History, failure analysis includes examination of past experience
- Databank of risk events that have occurred

An example of risks for a typical AFROSAI-E goal/objective is shown below.

	Goal/Objective Statement	Identified Risks
1	To provide timely and high quality audit services	• Low audit coverage • Poor quality of reports • Untimely reports

All the identified risks should be clustered so that a list of the main risks facing the SAI is drawn. It is recommended that the number of strategic risks should be kept to a minimum. Below are examples of strategic risks from some SAIs.

SAI A

Risks

1. Loss of independence *– independence underpins the value of the Auditor- General's products.*
2. Audit failure *– the risk that we issue an incorrect audit opinion with material impact, or a report that is significantly wrong in nature or process.*
3. Loss of capability *– the risk that we are unable to retain, recruit, or access people with the technical and other skills our audit work requires.*
4. Loss of reputation *– the risk that we may lose reputation or credibility that affects our ability to maintain effective relationships with stakeholders.*

SAI B

Risks

1. *Loss of stakeholder confidence*
2. *Fraud risk*
3. *SAI not achieving clean audit report*
4. *Continued organisational stability risk*
5. *Failure to achieve desired SAI culture/ transformation targets*

6.5 Identifying the causes

The process of identifying the risks should also include the causes. This is important because remedial action can only be taken if the reason for the occurrence of the risks is clear. Please find below a continuation of the example which now includes the causes.

	Goal/Objective Statement	Identified Risks	Causes
1	To provide timely and high quality audit services	- Low audit coverage - Poor quality of reports - Untimely reports	- Resistance to new methodology - Lack of guidance documents – Lack of audit tools - Inadequate training - Inadequate manpower - Inadequate knowledge of standards

Please refer to *appendix 2* for examples of strategic risks and their causes.

6.6 Identifying Operational Risks

Besides identifying risks to specific objectives (which would be operational objectives in this case).as illustrated above, it is also important to focus on the risks related to processes, systems and people.

Processes
These are the processes operated by the SAI. This includes the audit process, payments process, communications process, Human Resource processes etc.

Systems
This relates to the systems used to support the processes. Eg IT systems

People
The people employed by the SAI to help operate and manage the process. In fact major internal control failures are due to the failure of people.

All managers in the organisation should have good insights of their organisations and the functions that they are responsible for to enable them know their risks and to have necessary mechanisms to manage them.

Step 1. List the main functions or activities in the organisation. Identify the processes in the key functions to look at key process risks that must be managed.

Step 2. Select key functions and ascertain the main processes therein. In a SAI, for example, the following business processes exist:

Functions	Processes
Auditing	Overall Regularity and Performance Audit Plan, Pre-engagement, Audit Planning, Audit field work, Audit conclusions and reporting, quality control, follow up
Training	Needs assessment, course developments, training, follow up
Human Resource	Recruitment, Retention, Career development, Performance Management
Finance	Revenue/payments/accounting/budgeting
Store/ Registry	Procurement/Receipts/Issues/Custody and reporting
IT Support	Procurement/Maintenance/Disposal/Reporting

Step 3. Organise a meeting with each group to facilitate them to take stock of their risk areas existing in each of their processes.

- You may refer to recent incidents that have affected their operations.
- Use data analysis, business indicators, management reports, etc to look for other operational risks.

Step 4. For each of the functions, identify any risks with the process, systems, people, and any other factors.

Please refer to *appendix 2* for examples of operational risks and their causes.

6.7 Risk Register

The main output of the risk identification process is a list of identified risks. This will be documented in a risk register. A risk register is a document that contains the results of various risk management processes. It is often displayed in a table or spreadsheet format. The risk register is a key document in the SAI's risk management process. It forms part of the risk plan mentioned in chapter 4 and will also be used as a monitoring tool.

The risk register contains:

- An identification number for each risk.
- The name of each risk.
- The root cause of each risk.
- Assessment - the probability and impact of each risk occurring.

- The risk responses
- The control activities
- The risk owner or person who will take responsibility for each risk.
- The status of each risk

Please note that at this stage, only the first three columns that is, *number*, *risk* and *root cause* will be completed.

Sample Risk Register

No.	Risk	Root causes	Assessment			Risk Response	Control Activities	Risk Owner	Status
			Probability	Impact	Acceptable/ Unacceptable				
1.	Poor quality reports	- Lack of guidance documents – Lack of audit tools - Inadequate training - Resistance to new methodology							

CHAPTER 7

RISK ASSESSMENT

7.0 Introduction

After identifying the risks, the next step is to assess the risks. The objective of assessing risks is to identify which risks are important enough and significant enough to be the focus of management attention. This will allow the SAI to consider the extent to which potential risks have an impact on the achievement of objectives.

7.1 Risk assessment process

For each risk/threat identified the following must be addressed:

The impact / consequence - This is the potential magnitude of the impact on the SAI's objectives should the risk actually occur. This must be assessed on the basis that management have no specific controls in place to address the risk, i.e. without any controls in place, what will the impact of this risk be?

Using the examples from the previous chapter, the questions will be:

- What is the impact of low audit coverage?
- What is the impact of poor quality reports?
- What is the impact of untimely reports?

The probability of occurrence / likelihood - This is the likelihood that the identified risk will occur within a specified period of time (between 1 and 3 years) on the basis that there are no specific controls in place to address the risk. The questions for our risks will be :

- What is the likelihood of low audit coverage?
- What is the likelihood of having poor quality reports?
- What is the likelihood of untimely reports?

The steps that could be taken for the assessment and the tables that could be used are illustrated below:

Step 1 – Quantifying the parameters

The SAI should agree on the quantification system for both impact and likelihood before the assessment takes place. The two tables can be used to quantify impact and likelihood.

Impact

Rating	**Level**	**Outcome description**
5	Catastrophic	Disaster with potential to harm the SAI substantially
4	Major	Critical event which can be endured but which may have a prolonged negative impact and extensive consequences.
3	Moderate	Major events, which can be managed but requires additional resources and management effort.
2	Minor	Event, which can be managed under normal operating conditions.
1	Insignificant	Consequences can be readily absorbed under normal operating conditions.

Likelihood/Probability of occurrence

Rating	**Probability level**	**Description**
5	Almost certain	The event is expected to occur in most circumstances.
4	Likely	The event will probably occur in most circumstances.
3	Moderate	The event should occur at some time.
2	Unlikely	The event could occur at some time.
1	Rare	The event may occur only in exceptional circumstances.

Step 2 - Probability/impact matrix

A **probability/impact matrix** or **chart** lists the relative impact of the risk occurring on one side of a matrix or axis on a chart and the relative probability of a risk occurring on the other. The risk index will be a combination of the impact and likelihood – risk index = impact x likelihood. The results using the quantification in the two tables above will be applied in the table below in order to arrive the conclusion as to whether the risk is maximum, high, medium low or minimum as shown in the table below.

I	5	5	10	15	20	25
M	4	4	8	12	15	20
P	3	3	6	9	12	15
A	2	2	4	6	8	10
C	1	1	2	3	4	5
T		1	2	3	4	5
	LIKELIHOOD					

For example for the risk of low quality reports: if the impact is very high say 5 and the likelihood is high say 4 then the risk index will be 5*4=20.

Step 3 – Determine risk acceptance criteria

The SAI needs to determine the criteria for risk acceptance and tolerance. The most important risks which will require management focus will be those with a high impact and high likelihood of occurrence. The risk acceptability levels will also depend on the risk appetite of the SAI. If the SAI is risk averse, then even low levels of risk will not be acceptable. The table below which should be read in conjunction with the one above will be used to conclude on the assessment of the risk likelihood or impact.

RISK INDEX	RISK MAGNITUDE	RISK ACCEPTIBILITY	PROPOSED ACTIONS
20 – 25	Maximum	Unacceptable	Take action with highest priority – Head of SAI attention
15 – 19	High Risk	Unacceptable	
10 – 14	Medium Risk	Unacceptable	Take action to reduce risk
5 – 9	Low Risk	Acceptable	No risk reduction – control, monitor, inform management
1 – 4	Minimum Risk	Acceptable	No risk reduction – control, monitor, inform management

Using the example from above where the risk index was 20 then the risk magnitude would be *maximum* and risk acceptability *unacceptable*.

However it is also important that SAIs prepare themselves for relevant high – impact but low likelihood risks. This class of risks can have destructive consequences when they occur. An example of this could be ethical breaches by top management where the impact is very high but the likelihood very low.

7.2 Risk Register

The results of the risk assessment will be entered in the register.

No.	Risk	Root causes	Assessment				Risk Response	Control Activities	Risk Owner	Status
			Impact	Probability	Risk index	Acceptable/ Unacceptable				
1.	Poor quality reports	- Resistance to new methodology - Lack of guidance documents – Lack of audit tools - Inadequate training	5	4	20	Unacceptable				

7.3 Conclusion

This chapter has shown the process for assessing risks in relation to impact and likelihood which entails prioritizing high – impact and high – likelihood risks. However judgement should be used in dealing with high impact/ low likelihood risks.

CHAPTER 8

RISK RESPONSE

8.0 Introduction

After assessing the risk likelihood and impact, the SAI should consider its response that will bring the risk to a tolerable level. The risk responses will be linked to the SAI's risk appetite and the costs and benefits of potential risk responses. In some ways the process is similar to coming up with strategies for identified goals and objectives during the strategic planning process.

The ways to address identified risks include; risk transfer, risk reduction, risk avoidance and risk acceptance.

8.1 Important considerations

An important issue in considering response to risk is the identification of the "risk appetite" of the SAI. Risk appetite is the amount of risk to which the SAI is prepared to be exposed before it judges action to be necessary. Decisions about responses to risk have to be taken in conjunction with an identification of the amount of risk that can be tolerated. The risk appetite of an organisation will vary according to the perceived importance of the risks. For example, in a SAI environment, risks relating to ethical breaches cannot be tolerated.

8.2 Risk transfer

This is a risk mitigation strategy that involves shifting the risk to another entity. A number of SAIs actually apply this risk response strategy when they contract out work to private firms after identifying risks related to manpower and skills adequacies. However, it should be noted that not all risks can be transferred. When a SAI contracts out audit work, there is still need to ensure that the work has been done in accordance with the applicable standards.

Another example of a risk transfer strategy is if a SAI insures its buildings against fire or comprehensive insurance cover for its motor vehicles it will be using. The cost of transferring the risk in this manner must be carefully discounted against the potential costs of the risk and the probability of it materializing.

8.3 Risk reduction

This is the approach usually used by most SAIs to minimize risk. It refers to ways whereby the SAI institutes appropriate controls to manage the accepted risky position or exposure. This may involve improvements to existing methods and systems, changes in responsibilities, improvements to internal controls, etc.

Examples might include improving audit quality controls by:

- Improving the review process
- Introducing electronic working papers
- Introducing a quality assurance unit

8.4 Risk avoidance

This occurs when the SAI exits the activities giving rise to the risk. If there is no way that the given threat can be controlled or reduced and the possible risks outweigh the potential benefits then it advisable for the SAI to avoid the risk.

The following are examples of risk avoidance:

- The SAI decides to delay the introduction of a project like electronic working papers because of inadequate laptops
- Plans to decentralize are abandoned by the SAI because of logistical risks
- The restructuring process is stopped because of staff resistance

8.5 Risk acceptance

The risk acceptance is used mostly where no further economic, efficient and effective controls are possible given the SAI's defined risk appetite. Often, it may be better to accept the risk than to use excessive resources to eliminate it.

Examples in the SAI environment are as follows:

- SAI decides not to insure buildings and vehicles
- SAI accepts that it cannot report on time because of late submission of financial statements

8.6 Documenting Risk Responses

The risk responses will be included in the risk register..

The results of the risk assessment will be entered in the register.

No.	Risk	Root causes	Assessment			Risk Response	Control Activities	Risk Owner	Status
			Probability	Impact	Acceptable/ Unacceptable				
1.	*Poor quality reports*	*- Lack of guidance documents* *– Lack of audit tools* *- Inadequate training* *- Resistance to new methodology*	*4*	*5*	*Unacceptable*	*Risk reduction*			

CHAPTER 9

CONTROL ACTIVITIES

9.0 Introduction

Once the SAI has selected the preferred method of addressing the risk it needs an implementation plan. A critical part of any implementation plan is control activities.

9.1 What are Control Activities

Control activities are the procedures executed to address risks and to achieve the SAI's objectives. To be effective, control activities need to:

- be appropriate - that is, the right control in the right place and commensurate to the risk involved;
- function consistently according to plan - that is, be complied with by all employees involved and not bypassed when key personnel are away or the workload is heavy;
- be cost effective - that is, the cost of implementing the control should not exceed the benefits derived;
- be comprehensive, reasonable and directly relate to the control objectives.

9.2 Types of Controls

Control activities implemented by management can be divided into two categories (These are the categories used in the AFROSAI-E Regularity Audit manual. SAIs are free to use other categories) which are:

- preventative controls
- detective controls.

Please find table below with examples related to risks identified to ethics and independence of audit staff:

CONTROL	DEFINITION	EXAMPLE
Preventive	Preventive controls are designed to limit the possibility of a risk maturing and an undesirable outcome being realized.	Mandatory training sessions that include ethics, independence rules, and SAI policies and procedures.
Detective	Detective controls are designed to Identify whether undesirable outcomes have occurred after the event.	Random checks of compliance could be performed.

While there is room for all types of internal control procedures in a SAI, preventive controls are clearly the most useful. Although necessary in a good internal control system, detection of an independence violation after the fact is less desirable than prevention in the first place. Detective controls rarely work well as a deterrent in the absence of penalties. Once there is a suggestion that a SAI is lacking independence, a great deal of time and energy is spent answering those charges and rehabilitating the public image of the SAI. However, sometimes it takes longer to implement and can be more costly. In such cases a detective control can provide a temporary solution until the preventative control is implemented.

9.3 Risk Register

The control activities will be entered in the register.

No.	Risk	Root causes	Assessment			Risk Response	Control Activities	Risk Owner	Status
			Probability	Impact	Acceptable/ Unacceptable				
1.	*Poor quality reports*	*- Lack of guidance documents* *– Lack of audit tools* *- Inadequate training* *- Resistance to new methodology*	*4*	*5*	*Unacceptable*	*Risk reduction*	Develop manual Enhance review process Train on new methodology		

9.3 Conclusion

Control activities are key to risk management. In order to be effective, the functioning of the controls should continuously be monitored. This will be covered in the remaining chapters.

CHAPTER 10

INFORMATION AND COMMUNICATION

10.0 Introduction

Information and communication are prerequisites for an effective risk management system. Management needs to identify, capture, and communicate pertinent information in a form and timeframe that enables people to carry out their responsibilities.

Reference should be made to the AFROSAI-E Communication guideline for more details on communication in SAIs.

10.1 Information requirements

Information whether historical or current is key to effective risk management. Historical data allows the SAI to track actual performance against targets, plans and expectations and can provide early warnings of potential events that require management attention. Current data allows management to take a real-time view of existing risks within the SAI and identify variations from expectations. This can allow the SAI to determine whether it is operating within risk tolerances.

A good Management Information System is a pre-requisite to effective risk management. This will ensure that information is captured and is available to the relevant role players. This will also facilitate monitoring which is covered in the next chapter. It is also important that the risk register is updated timeously.

10.2 What should be communicated

Management provides information that addresses behavioural expectations and responsibilities of personnel. This should include a statement of the SAI's risk management philosophy and approach. Information about processes and procedures should align with and underpin the desired culture.

Communication should convey:

- The importance and relevance of SAI's risk management processes and procedures
- The SAI's objectives
- The SAI's risk appetite and risk tolerances
- A common language and process for identifying and assessing risks
- The roles and responsibilities of different personnel in effecting and supporting the components of risk management.

10.4 Methods of communication

As stated in earlier chapters, risk management is not a separate isolated event with its own separate structures unless when it is necessary. In most cases normal reporting lines are the appropriate channels of communication. However, there are some circumstances where alternative channels of communication such as, some form of whistle blowing is necessary for example for fraud or ethical breaches. In such cases the communication will need to be directed to management. This kind of alternative communication where staff can employ without fear of repercussion should also be available to external stakeholders. The seriousness in which communication with external stakeholders is taken and the honesty of such communication also sends important messages throughout the SAI and can have a significant impact on organisational culture.

10.5 Conclusion

Effective communication is essential to facilitate understanding of the extent to which risk is being managed leading to the achievement of the strategic and operational objectives.

CHAPTER 11

MONITORING

11.0 Introduction

Risk management should be monitored. Monitoring involves the assessment of both the presence and functioning of the components in risk management and the quality of their performance over time. This will ensure that risk continues to be managed at all levels and across the SAI. Monitoring can be done in two ways, that is, either through ongoing activities or separate evaluations.

11.1 Ongoing Monitoring

Ongoing monitoring is built into the normal, recurring operating activities of the SAI. This is more effective than separate evaluations which take place after the fact. Ongoing monitoring will keep track of any changes in the objectives of the SAI which might affect the portfolio of risks and risk responses.

11.2 Evaluations

The frequency of separate evaluations is a matter of management's judgement. The evaluations will vary in scope or frequency depending on the significance of the risks and the related responses and controls. Usually, some combination of ongoing monitoring and separate evaluations will ensure that risk management maintains its effectiveness over time.

11.3 Monitoring Tools

The risk register, management information system and periodic reports will be the main tools used to monitor the risk management responses. Other monitoring reports for strategic and operational planning will also be used. These processes should be built into the normal recurring activities of an SAI and include regular management and supervisory activities. Corrective actions taken in response to management's monitoring activities should be evident.

11.4 Role of Internal Auditors

The Institute of Internal Auditors (IIA) has developed the globally accepted definition of internal auditing, as follows: *Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*

It is clear from the above definition that internal auditors should play an important role in risk management, monitoring whether there are robust risks – management processes in place, and targeting internal audit resources to priorities based on the assessment. Internal auditors also support the development of the risk framework by obtaining thorough understanding of the organisation's objectives and maintaining a continuing dialogue with key stakeholders.

The risk framework needs to be challenged by internal auditors to maintain its relevance. Internal auditing should monitor key performance metrics to identify process and system volatility quickly and determine how best to obtain reasonable assurance that appropriate risk management is being affected.

11.5 Role of External Auditors

In accordance to ISSAI 1315, external auditors are required to identify risks during the process of obtaining an understanding of the entity and its environment. The auditors should assess the risk management process and the associated control activities.

11.6 Output

Any significant failings or weaknesses identified should be discussed, including the effect that they have had, or may have had, on the SAI, and the actions being taken to rectify them. The main outputs of risk monitoring are:

- *Requested changes* – these could be changes in risk portfolio, related responses or control activities.

- *Recommended corrective and preventive actions* - All risk management deficiencies that affect a SAI's ability to develop and implement its strategy and to achieve its established objectives should be reported to those positioned to take necessary action.

- *Updates the risk register* – for any changes resulting from the monitoring.

- *Risk Management reports* **–** these could be produced quarterly, bi-annually and annually.

Risk Register

The last column in the risk register: "*status*" will be used to monitor progress.

No.	Risk	Root causes	Assessment			Risk Response	Control Activities	Risk Owner	Status
			Probability	Impact	Acceptable/ Unacceptable				
1.	*Poor quality reports*	*- Lack of guidance documents* *– Lack of audit tools* *- Inadequate training* *- Resistance to new methodology*	*4*	*5*	*Unacceptable*	*Risk reduction*	Develop manual Enhance review process Train on new methodology	DAG	Done In progress 50% staff trained

11.7 Conclusion

Management needs to constantly monitor the effectiveness of their risk management system in order to determine whether it is still appropriate and effective.

APPENDIX 1: A GENERIC RISK MANAGEMENT POLICY FOR AN SAI

Purpose

The purpose of this document is to set out the SAI's Risk Management Policy and amongst other things it includes the following:

- The objectives of our Risk Management policy;
- Definitions of relevant terms;
- Risk management principles;
- Relative responsibilities;
- The Risk Framework and how it will work; and
- How Risk Management contributes to providing an Assurance.

Mission

The SAI exists to promote good governance, transparency and accountability in the management of public resources and reporting to Parliament.

Vision

The vision of SAI XYZ is to be a centre of excellence in public sector auditing.

Strategic Goals and Objectives

The overall objective of the SAI is to contribute to the efficiency of the public administration of government. The goals and objectives of the SAI as outlined in the current Strategic Plan for the period 2010 - 2015 are:

- To make the SAI independent and accountable
- To provide timely and high quality audit services
- To have an adequate and competent workforce
- To establish a modern and effective organisation and management system
- To enhance the image and impact of the SAI.

The Goals and Objectives of Risk Management

The objectives of this Risk Management policy are to assist management to make informed decisions which will;

- Improve the SAI's performance on decision making and planning;
- Provide a sound basis for integrated entity risk management and internal control as components of good corporate governance.

The improvements and benefits which effective Entity Risk Management should provide are;

- An increased likelihood of achieving the SAI's aims, objectives and priorities;
- Prioritising the allocation of resources;
- Giving an early warning of potential problems; and
- Providing everyone with the skills to be confident risk takers.

Definitions of Risk Concepts

The SAI will use the Committee of Sponsoring Organisations (COSO) of the Treadway Commission framework in defining risk and risk management. COSO defines risk as "…the possibility that an event can adversely affect the achievement of objectives." We define risk management as the identification and evaluation of actual and potential risk areas as they pertain to the SAI as a whole, followed by a process of either transfer, acceptance (tolerance) or reduction or avoidance of each risk.

Risk management shall be applied across the entire SAI to identify and manage potential risks that may have an adverse effect on the SAI's ability to achieve its strategic goals and objectives. Consequently, all managers shall take the necessary steps to identify, categorize and rank the risks the SAI is exposed to according to their likely impact with the aim of taking a decision(s) on how best the risks can be managed.

The risk philosophy reflects the SAI's values, influencing its culture and operating style, and affects how well fiscal programs can be implemented, maintained, and controlled. Risk appetite is the residual risk the SAI is willing to accept or tolerate in seeking to achieve its objectives. Once a year the Auditor General will determine the levels of risk tolerance by setting rules or directives for risk taking in respect of all types of risks the SAI will be facing.

The SAI's Risk Management Principles

Risk management should be a central part of the SAI's strategic management process. The principles contained in this policy and strategy will be applied at both strategic and operational levels within the SAI. The implementation of this policy requires that our internal control environment is developed and established. All managers shall lead by example and abide by the SAI's Code of Conduct. Managers should be guided by the SAI's vision, mission and strategic objectives as the basis for the development

and implementing the risk management process. Risk management is an integral part of every process within the SAI and is the responsibility of everyone within the SAI.

Prior to finalizing strategy, management must ensure that the SAI strategy is within its overall risk appetite unless the strategy requires the overhauling of the existing risk management policy. It is for this reason that the development of risk management in an SAI should grow in harmony with the development of the SAI.

All risk management activities will be aligned to SAI goals, objectives and the SAI priorities, and aims to protect and enhance the reputation and standing of the SAI. Risk analysis will form part of the SAI strategic planning, operational planning and business unit planning procedures.

Our risk management approach will inform and direct our work to gain an assurance on the reliability of the SAI systems. Managers and staff at all levels will have the responsibility to identify, evaluate and manage or report risks, and will be equipped to do so.

We will foster a culture which provides for spreading best practice, lessons learnt and expertise acquired from our risk management activities across the SAI for the benefit of the entire organisation.

Principles for Managing Specific Risks

Risk Management in the SAI should be proactive and reasoned. Strategic and operational risks should be identified, objectively assessed, and, where this is the appropriate response, actively managed. The aim is to anticipate, and where possible, avoid risks rather than dealing with their consequences. However, for some key areas where the likelihood of a risk occurring is relatively small, but the impact is high, we may cover that risk by developing Contingency Plans.

In determining an appropriate response, the cost of control/risk management, and the impact of risks occurring will be balanced with the benefits of reducing and or managing risk. This means that we should not necessarily set up and monitor controls to counter risks where the cost and effort are disproportionate to the impact or expected benefits. We also recognise that some risks can be managed by transferring them to a third party, for example by contracting out audits or taking insurance.

Roles and Responsibilities

The total process of risk management, which includes a related system of internal controls, is the responsibility of the Auditor General (AG). Management is accountable to the AG for designing, implementing and monitoring the process of risk management and integrating it into the day to day activities of the SAI. Management is also accountable to the AG for providing assurance that it has done so. The internal audit function should be used to provide independent assurance in relation to management's assertions surrounding the effectiveness of risk management and internal control.

Although management may appoint a risk officer or risk champion to assist in the execution of the risk management process, the accountability to the AG remains with management and should be the responsibility of every employee. The risk management process does not reside in any one individual or function but requires an inclusive team-based approach for effective application across the SAI. To assist him/her in the discharge of his/her duties and responsibilities, the AG may appoint a dedicated Risk Management Committee to review the risk management process and the significant risks facing the SAI.

The Risk Management Committee is responsible for coordinating and monitoring compliance with the SAI internal controls i.e. Policies, the SAI's Standard Operating Procedures, Code of Conduct, applicable legislation etc. and by obtaining and analysing all major risk assessment documents/risk registers.

Risk assessment should be carried out at a strategic and operational level. The strategic risk assessment is carried out by Top Management at least once a year before the commencement of a strategic or business planning cycle. Operational risk assessment is carried out by individual business units and functions at least once a year preferably at the beginning of the audit cycle.

The risk coordinator or champion monitors and reports on key organisational risks to top management and the Risk Management Committee.

Monitoring will occur through regular updates of internal control monitoring processes. Internal audit will also provide a support and feedback mechanism for monitoring risks through risk based internal audits. This committee should consider the risk strategy and policy and should monitor the process at operational level and the reporting thereon. The committee to the extent that it is concerned with risk management, should consider the results of the risk management and internal control processes and the disclosure in the annual report.

Internal audit should not assume the functions, systems and processes of risk management but should assist the AG and management in the monitoring of the risk management process. The responsibilities of the AG, management; the Risk Management Committee; staff and Internal Audit are set out below:

Detailed Roles and Responsibilities Table

The following risk management roles and responsibilities shall be observed and complied with by all staff across the SAI:

Auditor General and Deputy Auditors General:

- Establish the SAI's risk management philosophy, its risk tolerance levels (appetite) and ensure the integration of risk management in all the SAI processes.
- Exercise the broad risk management strategy and oversight for the SAI
- Determine strategic approach to risk
- Assess the system and structure for risk management
- Identify and understand the most significant risks
- Manage the SAI when in a crisis

Senior and Operational managers:

- Build risk aware culture within the unit(s)
- Agree risk management performance targets
- Ensure implementation of risk improvement recommendations
- Identify and report changed circumstances / risks
- Identify and recommend possible risk management topics for further training
- Implement risk management strategies and plans

Individual Employees:

- Understand, accept and implement risk management processes
- Report inefficient, unnecessary or unworkable controls
- Report loss events and near miss incidents
- Co-operate with management on incident investigations

Risk Management Committee:

- Assist the SAI in establishing risk policies and risk training interventions
- Review or Develop the risk management policy and plans and suggest changes
- Document the internal risk policies, structures and plans
- Coordinate the risk management (and internal control) activities
- Supervises the maintenance of the risk register
- Reviews the quarterly risk management monitoring reports
- Compile risk information and prepare reports for the Auditor General.

Risk Coordinator or Champion:

- Maintains the risk register
- Coordinates the gathering of possible risk information
- Drafts the quarterly risk management monitoring reports
- Develop specialist contingency and recovery plans
- Keep up to date with developments in the specialist area
- Support investigations of incidents and near misses

Internal Audit Manager:

- Develop a risk-based internal audit programme
- Audit the risk processes across the organization
- Receive and provide assurance on the management of risk
- Report on the efficiency and effectiveness of internal controls

Risk Tolerance

The AG and management should encourage the taking of controlled risks, the grasping of new opportunities and the use of innovative approaches to further the interests of the SAI and achieve its objectives provided the resultant exposures are within the SAI's risk tolerance range. The SAI's Risk Tolerance can be defined by reference to the following components.

Acceptable risks

All personnel should be willing and able to take calculated risks to achieve their own and the SAI's objectives and to benefit the SAI. The associated risks of proposed actions and decisions should be properly identified, evaluated and managed to ensure that exposures are acceptable.

Within the whole SAI, particular care is needed in taking any action which could;

- *Impact on the reputation of the SAI* - the risk that we may lose reputation or credibility that affects our ability to maintain effective relationships with stakeholders
- *Impact on performance resulting in audit failure* - the risk that we issue an incorrect audit opinion with material impact, or a report that is significantly wrong in nature or process.
- *Undermine independent and objective review in carrying out audit work* - independence underpins the value of the Auditor-General's products.

- *Impact on organizational capability* – the risk that we are unable to retain, recruit, or access people with the technical and other skills our audit work requires and inability to access other resources

Any threat or opportunity which has a sizeable potential impact on any of the above should be examined, its exposures defined and it should be discussed with the appropriate line manager. Where there is significant potential impact and high likelihood of occurrence it should be referred to the Risk Management Committee.

Risk Framework

The COSO Risk Management Framework approach shall be the model applied throughout the SAI. The SAI will maintain a Risk Register as a basis for implementing and monitoring the risk management activities. This register will include details of the Impact and Likelihood of each of the risks identified, indicate Ownership/Responsibility and specify an Activity/Action Plan for treatment. This will be reviewed and updated yearly. Progress of the risk management programme will be a standing top management meeting agenda item.

To help to meet their responsibilities to identify, evaluate and manage operational risks, Business Unit Managers should maintain:

- An Divisional/Business Unit Risk profile which details the priority (impact and likelihood) and ownership within the Division/Business unit;
- A risk management action plan based on the SAI's Annual risk plan;
- Evidence of regular reviews and monitoring of the profile and action plan, e.g. minutes of committee/divisional/ sectional unit meetings.

Assurance

The use of the COSO risk management approach should help to identify areas of great concern for a detailed review. The SAI's Risk Register will assist Internal Audit unit to direct its limited resources to those areas of great concern. For the SAI risks identified by management, internal audit will evaluate the effectiveness of the existing controls and risk management responses. The internal audit assurance will include an assessment of the reliability and effectiveness of the SAI's overall Risk Management programme.

EVALUATION AND REPORTING

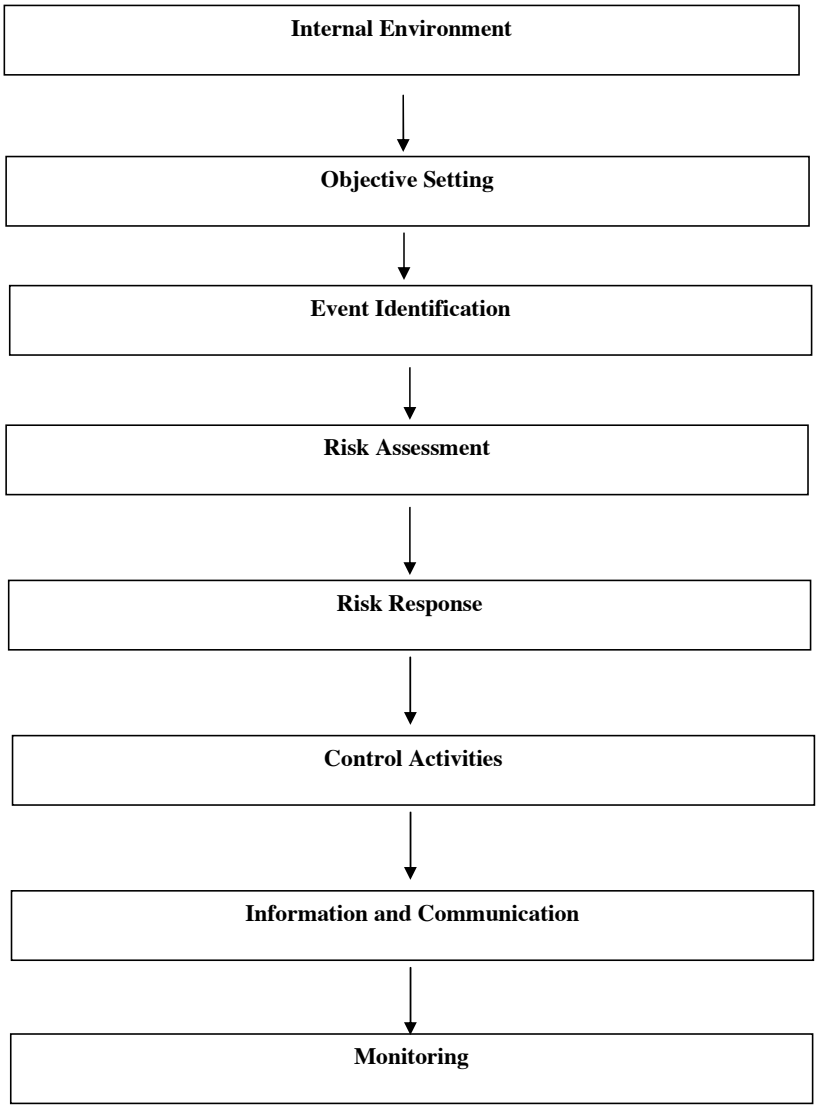
This process includes monitoring and reviewing identified risks, and being open to new or changed risks and opportunities resulting from evolving circumstances.(Refer to details on step 8 below) All risks that have be classified as high impact should be reported to the Risk Committee via the responsible Senior Manager. As these risks will require further analysis before they are reported to top management, the reports should be forwarded to the Risk Coordinator or Champion as soon as possible.

The SAI risk register is monitored by top management on a quarterly basis, and maintained by the Risk Coordinator or Champion.

THE RISK MANAGEMENT PROCESS OF THE SAI

The SAI's adopted risk management process is based on the COSO–ERM model as illustrated in the diagram below:

Figure 4: The Eight Components COSO Risk Management Process



STEP 1 - OBJECTIVES SETTING

Objectives must be established before management can identify and assess risks to their achievement and take the necessary actions to mitigate those risks.

There will be no separate objective setting process for risk management process. The strategic objectives will be obtained from the strategic plan and the annual operational plan will be used to identify the annual objectives and key functions of the SAI.

The risk management philosophy, culture, integrity, values and organizational structure will affect the setting of objectives. Another key consideration in objective setting is the risk appetite.

STEP 2 - RISKS IDENTIFICATION

Risk identification involves identifying potential events, occurring internally or externally, that could affect achievement of objectives. It addresses how internal and external factors combine and interact to influence the risk profile.

Top and senior management of the SAI will be involved in the identification of strategic risks while senior and operational managers will be involved with operational risks. Other participants in risk identification activities can include, where appropriate: team members, risk management team, the SAI's quality assurance function, subject matter experts, and stakeholders

Risk identification will be linked to the strategic planning process. During strategic planning, the risk identification process will already start as the SAI conducts the needs assessment or the situational analysis. However since the process is based on established objectives, the process can only be finalized after identifying the goals/objectives of the SAI.

The risk identification process will include both internal and external factors.

The following methods will be used to identify risks:

- Interview /focus group discussions- for example gather together top and senior management to brainstorm on possible risks to achievement of objectives on different levels.
- Survey, questionnaire
- SWOT analysis
- History, failure analysis includes examination of past experience
- Databank of risk events that have occurred

All the identified risks will be recorded in the risk register which will contain the following information:

- An identification number for each risk.
- The name of each risk.
- The root cause of each risk.
- Assessment - the probability and impact of each risk occurring.
- The risk responses
- The control activities

- The risk owner or person who will take responsibility for each risk.
- The status of each risk

STEP 3 - RISK ASSESSMENT

The objective of assessing risks is to identify which risks are important enough and significant enough to be the focus of management attention. This will allow the SAI to consider the extent to which potential risks have an impact on the achievement of objectives.

For each risk/threat identified the following must be addressed:

- *The impact / consequence* - This is the potential magnitude of the impact on the SAI's objectives should the risk actually occur.
- *The probability of occurrence / likelihood* - This is the likelihood that the identified risk will occur within a specified period of time (between 1 and 3 years) on the basis that there are no specific controls in place to address the risk.

The following steps will be used to assess risks:

1 – Quantifying the parameters

The two tables below will be used to quantify impact and likelihood.
Impact

Rating	**Level**	**Outcome description**
5	Catastrophic	Disaster with potential to harm the SAI substantially
4	Major	Critical event which can be endured but which may have a prolonged negative impact and extensive consequences.
3	Moderate	Major events, which can be managed but requires additional resources and management effort.
2	Minor	Event, which can be managed under normal operating conditions.
1	Insignificant	Consequences can be readily absorbed under normal operating conditions.

Likelihood/Probability of occurrence

Rating	Probability level	Description
5	Almost certain	The event is expected to occur in most circumstances.
4	Likely	The event will probably occur in most circumstances.
3	Moderate	The event should occur at some time.
2	Unlikely	The event could occur at some time.
1	Rare	The event may occur only in exceptional circumstances.

2 - Probability/impact matrix

The **probability/impact matrix** below will be used to calculate the risk index. The risk index will be a combination of the impact and likelihood – risk index = impact x likelihood. The results using the quantification in the two tables above will be applied in the table below in order to arrive at the conclusion as to whether the risk is maximum, high, medium low or minimum as shown in the table below.

I	5	5	10	15	20	25
M	4	4	8	12	15	20
P	3	3	6	9	12	15
A	2	2	4	6	8	10
C	1	1	2	3	4	5
T		1	2	3	4	5
	LIKELIHOOD					

For example for the risk of low quality reports: if the impact is very high say 5 and the likelihood is high say 4 then the risk index will be 5*4=20.

3 – Determine risk acceptance criteria

The SAI needs to determine the criteria for risk acceptance and tolerance. This will enable the SAI to focus on the most important risks which require management focus i.e. those with a high impact and high

likelihood of occurrence. The table below which should be read in conjunction with the one above will be used to conclude on the assessment of the risk likelihood or impact.

RISK INDEX	RISK MAGNITUDE	RISK ACCEPTIBILITY	PROPOSED ACTIONS
20 – 25	Maximum	Unacceptable	Take action with highest priority – Head of SAI attention
15 – 19	High Risk	Unacceptable	
10 – 14	Medium Risk	Unacceptable	Take action to reduce risk
5 – 9	Low Risk	Acceptable	No risk reduction – control, monitor, inform management
1 – 4	Minimum Risk	Acceptable	No risk reduction – control, monitor, inform management

Using the example from above where the risk index was 20 then the risk magnitude would be *maximum* and risk acceptability *unacceptable*.

The results should be entered in the risk register.

STEP 4 - RISK RESPONSE

After assessing the risk likelihood and impact, the next step would be to consider the response that will bring the risk to a tolerable level. The SAI will use four ways to address identified risk which are risk transfer, risk reduction, risk avoidance and risk acceptance.

Risk transfer

This is a risk mitigation strategy that involves shifting the risk to another entity e.g. contracting out audit work.

Risk reduction

This will be used when the SAI wants to respond by instituting appropriate controls to manage the accepted risky position or exposure. This may involve improvements to existing methods and systems, changes in responsibilities, improvements to internal controls, etc. It is foreseen that this will be the main response strategy for the SAI.

Risk avoidance

This will be applied if there is no way that the given threat can be controlled or reduced and the possible risks outweigh the potential benefits then it advisable for the SAI to avoid the risk.

Risk acceptance

The risk acceptance will be used mostly where no further economic, efficient and effective controls are possible given the SAI's defined risk appetite.

Documenting Risk Responses

The risk responses should be included in the risk register.

STEP 5 - CONTROL ACTIVITIES

Once the SAI has selected the preferred method of addressing the risk it needs an implementation plan. A critical part of any implementation plan is control activities. Control activities are the procedures executed to address risks and to achieve the SAI's objectives.);

The SAI will have two categories of control activities which are:

- preventative controls
- detective controls.

In order to be effective, the functioning of the controls should continuously be monitored.

STEP 6 - INFORMATION AND COMMUNICATION

Information and communication are prerequisites for an effective risk management system. All information related to risk management should be captured and communicate a form and timeframe that will enable staff to carry out their responsibilities. The SAI's Management Information System will be used as a tool to ensure that the information is captured and is available to the relevant role players.

STEP 7 - MONITORING

Monitoring will involve the assessment of both the presence and functioning of the components in risk management and the quality of their performance over time. This will ensure that risk continues to be managed at all levels and across the SAI.

Monitoring will be done in two ways, that is, either through ongoing activities or separate evaluations.

Ongoing Monitoring

Ongoing monitoring is built into the normal, recurring operating activities of the SAI. This is more effective than separate evaluations which take place after the fact. Ongoing monitoring will keep track of any changes in the objectives of the SAI which might affect the portfolio of risks and risk responses.

Evaluations

Comprehensive evaluations will be done annually. The risk Committee will be responsible for the comprehensive evaluations.

Role of Internal Auditors

Internal auditors will play an important role in risk management, monitoring whether there are robust risk – management processes in place. Internal audit resources will be prioritized on high risk areas. Internal auditors also support the development of the risk framework by obtaining thorough understanding of the organisation's objectives and maintaining a continuing dialogue with key stakeholders.

Output

Any significant failings or weaknesses identified should be discussed, including the effect that they have had, or may have had, on the SAI, and the actions being taken to rectify them.
The main outputs of risk monitoring will be:

- *Requested changes* – these could be changes in risk portfolio, related responses or control activities.
- *Recommended corrective and preventive actions* - All risk management deficiencies that affect a SAI's ability to develop and implement its strategy and to achieve its established objectives should be reported to those positioned to take necessary action.
- *Updates the risk register* – for any changes resulting from the monitoring.
- *Risk Management reports* **–** these could be produced quarterly, bi-annually and annually.

Appendix 2: Examples of Strategic Risks

RISK FACTORS	CAUSES
SAI's independence gets impaired	➢ Obsolete legal framework ➢ The Head of the SAI's is not in accordance with INTOSAI standards ➢ The SAI does not have discretion to choose its topics for audit purposes ➢ The SAI does not have financial autonomy ➢ The SAI does not have full access to information ➢ Lack of accountability, independence, transparency due to bias reporting, inadequate coverage, political intervention, abuse, etc ➢ Lack of trustworthiness of the SAI by stakeholders e.g. of wrong audit conclusions. ➢ Poor quality of service ➢ No commitment for audit quality ➢ Lack of qualified staff or poor human resource management ➢ No audit methodology being used or if used not consistently being applied. ➢ Political fear ➢ No proper auditing and accounting standards being used. ➢ Lack of financial resources ➢ Lack of audit tools and facilities available ➢ Lack of support from auditees
Reputational risk that SAI is perceived not to be transparent and much accountable.	➢ The activities of the SAI are not being independently scrutinized. ➢ Lack of credibility on audit reports, e.g. expected by donor agencies for utilization of funds. ➢ No peer review of the SAI activities;
Risk of bad governance	➢ SAI does not have any strategic plan and operational plan ➢ SAI's organisation structure is not much aligned to its strategic plan ➢ SAIs and its members are not committed to be compliant with Acts, regulations, code of ethics ➢ No annual reports of the SAIs and audited by an independent auditor; ➢ No audit committee ➢ No internal audit ➢ No risk management committee ➢ No effective board of management ➢ SAI is not being lead by example ➢ No transparent committee ➢ SAI does not have a Management Information System ➢ SAI does not have a computerized accounting system or an ERP ➢ SAI does not have an effective system of delegation
SAI is not responsive to changing environments and stakeholders' expectations	➢ No risk management framework ➢ No proper human resource development strategy in the SAI as to annual CPD hours requirements, career development, investment in training ➢ No research and developments in the SAI to encourage innovation and

	improvements ➢ Lack of networking with other SAIs and professional firms
Risk of non compliance with code of ethics	➢ No commitment to adhere to SAI's code of ethics
Risk of putting the reputation of the SAI at stake.	➢ Delays to submit its reports on the affairs of the Government or other parastatal bodies or local authorities ➢ Political affinity ➢ Audit works not being adequately supervised
Risk that SAI is not giving sufficient assurance to the public and other political leaders that value for money is being obtained	➢ Value of money is not gained from the audit work done on regularity audit, performance audit, environmental audit, transversal audit, IT audit etc being done. ➢ Vacant posts not filled since long ➢ SAI does not have a retention policy or career path for qualified and experienced staff,
Risk of not much contributing to improving governance in public sector	➢ Limiting its audit works to its statutory mandate and is not keeping itself with international trends ➢ Value of money is not gained from the audit work done on regularity audit, performance audit, environmental audit, transversal audit, IT audit etc being done. ➢ Lack of committed, experienced and professional people ➢ High level of staff turnover ➢ Inadequate resources as IT facilities like electronic working papers, CAATs.
Risk of audit reports not being accessible, understandable, to meet users expectations	➢ The SAI does not have any website to publicise its report ➢ SAI does not have a policy document on communicating to external stakeholders like the press ➢ The SAIs reports do not get much press coverage. ➢ The report of the SAI is more of a technical language that is difficult to be understood. ➢ SAI reports do not include enough recommendations ➢ The SAI reports are not much discussed at Parliamentary level.
Risk that the Parliament, responsible for good Governance of public funds not being able to discharge their responsibilities due to the SAI	➢ SAIs do not submit timely reports ➢ Auditees not being regulated and disciplined to submit their financial statements promptly and in compliance with necessary accounting standards and regulatory compliance. ➢ Inadequate audit coverage by the SAI ➢ The Public Accounts Committee has a backlog to deal with the SAI's audit reports
Risks that SAIs do not follow up its own findings and recommendations and provide assurance on the status of recommendations	➢ Inadequate follow up actions with clients management ➢ Past audit findings were not reconsidered and reported ➢ SAIs not fully committed to bring improvements and reforms in the public sector SAIs do not adequately partner with auditees, support networking and continuous education to bring improvements in the public sector.

Appendix 3 : Examples of Operational Risks

RISK FACTOR	RISKY EVENTS THAT ARE LIKELY TO OCCUR	CAUSES
Processes and systems	➢ Regular System Failure ➢ Complaints ➢ Long queues to process transaction ➢ Security breaches ➢ Equipment failure ➢ Data theft ➢ Destruction of systems	➢ Outdated/obsolete systems ➢ Lack of qualified personnel ➢ Lack of finance to invest ➢ Lack of maintenance and proper system support ➢ System lack Integrity ➢ Inadequate controls in systems ➢ Non development of systems and implementation failure ➢ Insufficient systems capacity ➢ Poor data integrity ➢
People	➢ Errors ➢ Internal fraud ➢ Employment fraud ➢ Employer's liability ➢ Absence / loss of key staff ➢ Wrongful trading	➢ Lack of control; ➢ Lack of segregation of duties; ➢ Insufficient skills, training, management or supervision; ➢ Unauthorised activity; ➢ Lack of integrity and honesty; ➢ Reliance on key personnel; ➢ Controls can be circumvented by collusion between two or more people; ➢ Management can override controls. ➢ Lack of customer focus and professionalism; ➢ Changes in organisational culture ➢ Lack of motivation;
External factors (Consider PEST also)	➢ Business interruption ➢ Third party theft ➢ External fraud ➢ Non compliance with standards ➢ Changes in regulatory standards ➢ Contractual failures	➢ Acts of God as natural disasters ➢ External criminal activities ➢ Political unrest ➢ Political factors can even change core objectives in short period of time. ➢ The regulatory, legal, tax, and business environment and any changes in that environment ➢ Exchange rates ➢ Interest rates and monetary policy of government

References

1. Auditor General of Eritrea's Draft Risk Management Policy 2010
2. Auditor-General of Mauritius' Draft Risk Management Policy 2010
3. AFROSAI-E Regularity Audit Manual 2010 & AFROSAI-E Performance Audit Manual 2010.
4. Australian/New Zealand Standards: Risk Management (AS/NZS 4360:2004)
5. Basel Committee on Banking Supervision. April 2005. Compliance and compliance Function in banks.
6. COSO's Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organisation of the Treadway Commission (COSO), New York, NY, September 2004 (see www.coso.org)
7. Cruywagen, Gert – Jungle Risk Management – Risk Lessons from the African Bush, Actua Press, 2008
8. Guidelines for Managing Risk in the Australian Public Service (1996)
9. INTOSAI Development Initiative (IDI)/ AFROSAI-E Strategic Planning – *A Handbook for Supreme Audit Institutions, 2009*.
10. International Organisation of Supreme Audit Institutions (INTOSAI) GOV 9100 – *Guidelines for Internal Control Standards for the Public Sector – 2004*
11. International Organisation of Supreme Audit Institutions (INTOSAI) GOV 9130 *Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management – 2004*
12. International Federation of Accountants (IFAC) – *Guide to Practice Management for Small and Medium –sized Practices: June 2010*
13. Institute of Directors – King III Report on Corporate Governance for South Africa, September 2009
14. International Standards Organisation – Draft Standard on Risk Management ISO 31000, 2008
15. The Committee of Sponsoring Organisation of the Treadway Commission (COSO), September 2004. *Enterprise Risk Management – Integrated framework*.
16. The Institute of Internal Auditors(IIA) – Role of Internal Auditors in Enterprise Risk Management
17. National Treasury Office of the Accountant General of South Africa – *Final Risk Management Framework for the Public Sector*
18. Risk and Compliance Management Framework for the Auditor –General of South Africa, 2010