THE STATE OF ERITREA
OFFICE OF THE AUDITOR GENERAL

Risk Management Policy

Introduction

All public sector organisations face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to provide efficient service for the public. Risk management enables management to effectively deal with uncertainty. As in all organisations, the Office of the Auditor General (OAG), although not exhaustive, faces some of internal and external risks which can be depicted as follows:-

Core Business Risks:
- Technical risk – failure to keep pace with technical developments, or investment in an inappropriate or inadequate/non-sustainable service plans to maintain continuity of service.
- Inadequate skills or resources to deliver services for government agencies
- Non-compliance with methodological and ethical standards.
- Audit complexity is greater than in house competence.
- Limitations of audit scope (audited entity not providing information requested).
- Increase in audits backlogs.
- Impact and/or change to auditing, accounting standards
- Government policy changes

Corporate Functions Risks
- Planned resources are not realized (personnel and budget)
- Government policy changes
- Technology related risks
- Human resource management risks
- Inadequate skills
- Limitations in delivering training

All these risks may result to the hindrance of providing effective and efficient service and eventually to loss of reputation of the OAG. It is therefore imperative to have risk management policy in place to enable management to effectively deal with uncertainty and its associated risks in order to comply with auditing standards and best practices and thereby the OAG is looked upon with trust, confidence and credibility by the public.

Mission

The mission of the Office of the Auditor General of the State of Eritrea is: "**To provide reasonable assurance in the management of public resources by our independent and objective public sector audit services.**"

Vision

The vision of the Office of the Auditor General of the State of Eritrea is: " **To be an independent, efficient and effective audit institution that promotes public accountability and transparency.**"

1. Title

Risk Management policy of the Office of the Auditor General.

2. Purpose

The OAG is committed to building increased awareness and a shared responsibility for risk management at all levels of the Office. The risk management practices of OAG are specifically designed to identify and assess all types of risks to the OAG, and to implement appropriate risk management techniques to enable it accomplish its mission. It is the aim of this Risk Management Policy to assist in the identification and evaluation of risks, to facilitate the selection and application of the best risk management techniques to mitigate risks, and to monitor the results. This policy is intended to ensure that:-
- risks to the OAG are identified, analyzed, and managed so that they are maintained at acceptable levels to enable the OAG conduct its works effectively and efficiently to the best of public interest;
- risks to the confidentiality, integrity, and availability of OAG information are considered in decision making processes;
- the OAG will manage risks to protect both the OAG staff and its assets and will maintain a proactive, long-term and sustainable risk management strategy;
- the policy explains the OAG's underlying approach to risk management. It gives key aspects of the risk management process, and identifies the main reporting procedures.

3. Scope

This policy covers internal and external environmental factors of risks that include:-
- *The OAG's risk management philosophy* - that influence culture and operating style including how risks are identified, the kind of risks accepted and how they are managed.

- ***Integrity and ethical values***- this is management's ethical value. The OAG's good reputation is so valuable; the standards of behaviour must go beyond mere compliance with minimum standard requirements.

- ***Code of conduct***- which are important to and the foundation of the promotion of an appropriate ethical tone.

- ***Professional competence of staff***- reflects the knowledge and skills needed to perform assigned tasks.

- ***Staffing/assignment of authority and responsibility*** - involves the degree to which individuals and teams are authorised to and encouraged to use initiative to address issues and solve problems.

- ***Risk appetite***- the amount of risk on a broad level that the OAG is willing to accept in seeking to achieve its objectives.

- ***Political neutrality***- independence from political influence in order to discharge professional responsibilities in an impartial way.

This policy is applicable to all areas of the OAG, including;
- Audit Departments
- Corporate function Divisions

4. Policy objectives

The Risk Management policy has been created to:-
- protect the OAG from those risks of significant likelihood and consequence in the pursuit of its stated strategic goals and objectives (as stated in OAG's Strategic Plan 2007-2011);

- provide a consistent risk management framework in which the risks concerning the functions of the OAG will be identified, considered, and addressed in key approval, review and control processes;

## 5. Approach to Risk Management

The approach to risk management set out in this Policy, will be approved by the Risk Management Committee (RMC) and the Auditor General. The approach allocates responsibility for risk management and establishes a framework within which risks are identified and evaluated so that an appropriate response can be determined and applied.

Risk management, therefore, involves a planned and systematic approach to the identification, assessment and mitigation of the risks that could hinder the

achievement of strategic objectives. The OAG's risk management process involves the following main steps:

- identifying the key strategic risks that would prevent achievement of objectives

- evaluating the significance of each risk

- identifying suitable responses to each risk

- devising mechanisms that help manage the risks

- regular review of risks.

This approach can be summarized diagrammatically as follows:
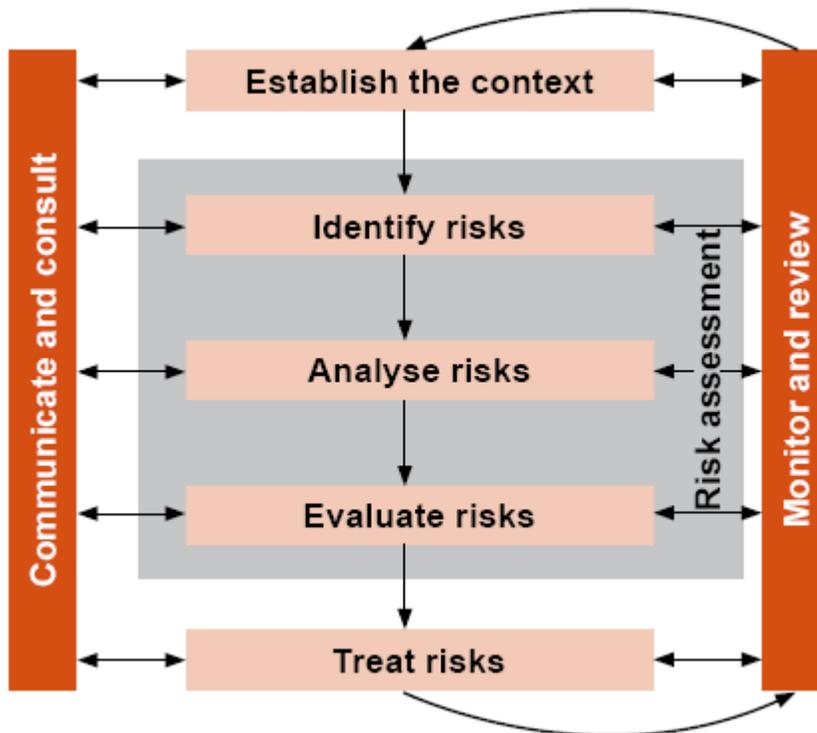
Source: *Australian and New Zealand Risk Management Standard*, AS/NZS 43 0:2004.

5.1. Identify the key strategic risks that would prevent achievement of objectives-

Top management and RMC are involved and committed to the identification of key risks. Risk identification should be supported by top, middle, lower management and all staff equally, as they all have an important role to play. Active commitment from the top down is necessary for effective risk identification.

5.2. Evaluate seriousness

The root cause of the risks identified should be analyzed and be assessed on the likelihood of occurrence and the potential impact on the strategic aims and objectives of the OAG should they be realized. Identified risks which pose a potentially major impact to the OAG are evaluated by the RMC in conjunction with the departments as appropriate. Risks must be evaluated from two perspectives – impact and likelihood – using a combination of quantitative and qualitative techniques based on the following criteria:

- Frequency of Exposure – How often the event or activity takes place
- Probability – The actual chance of a loss of trained and qualified staff, information leakage and undue influence of others to override professional judgments.
- Severity – The seriousness of the risk to OAG mission.

Once risks have been assessed the risk priorities should emerge. If the risk exposure is unacceptable given the risk appetite of the OAG, the risk should be classed as high priority or "key risk".

5.3 Identify Risk Response (Risk Control Techniques)

The responsibility of identifying and implementing the control measure(s)/procedures is that of the RMC and the Department Heads that control the activity presenting the risk exposure. They determine the method of control that provides the most effective means of risk reduction without compromising the mission of the OAG. The risks can be mitigated in a variety of ways including but not limited to:

- Preventing/controlling risks through staff training and supervision
- Redesigning processes and systems

5.4 Monitor and evaluate results

Upon implementation of the best risk management technique or combination of techniques, monitoring and evaluating the effectiveness and efficiency of the technique will be done by RMC and Department Heads to determine appropriateness and whether any changes and/or modifications of techniques should be made.

An annual report is prepared by the RMC as a basis for evaluating the overall effectiveness of the Risk Management Policy. This evaluation process is intended to ensure that the Risk Management Policy remains effective and, thus, reduces the OAG's exposure to foreseeable risks.

5.5 Regular review

RMC and Department Heads continually review the OAG's policy and monitor OAG activities to ensure that the goals of the Risk Management Policy are achieved. The key risks should be given regular attention at all times.

To coordinate the risk management process, this approach will combine oversight by the RMC, top Management and the Auditor General.

6. Key Principles

The following key principles outline the OAG's approach to risk management:

- A key objective of risk management is the development of a comprehensive risk management framework to ensure that risks are being managed in an efficient, effective, and economic manner. The framework will include risk management standards and risk assessment criteria:

- The risk appetite of OAG will emanate from the Strategic Plan.

- RMC will be responsible for providing annual assurance to the Auditor General on the adequacy of risk management.

- Department Heads and staff at all level are responsible for the management of all risks within their areas of control, including ensuring that appropriate systems are created to identify, assess, manage and review risks in line with the OAG Risk Management process.

7. Responsibilities

The implementation of the OAG Risk Management Policy is a responsibility shared by all audit and support staff. Department Heads, Directors, Senior Auditors, Team leaders, Auditors at all levels and support staff shall be responsible for comprehensive risk management of their respective activities. One of the core requirements of this policy will be the establishment of Risk Management Committee. A Committee appointed by the Auditor General will be responsible for oversight and assurance of the processes for the identification and assessment of the risk management process. Toward that end, the OAG's approach to risk management will embody the following principles:

- Risk Management will be embedded in all management systems.

- The identification and management of risk is the responsibility of all managers and staff throughout the OAG.

- The Committee will review the effectiveness of risk management systems regularly, and the results will be communicated to the Auditor General.

- Management should routinely identify and evaluate the risk to the achievement of OAG objectives. This would include the regular assessment of both the significance and the likelihood of occurrence of the risks arising.

- Having assessed the significance and likelihood of the risks arising, RMC should establish a Risk Prioritization program that assist in addressing higher priority items.

- Higher priority items are those risks judged to be both significant and have a high likelihood of occurrence. These risks are judged to be prime threats to the OAG and should be addressed at their source.
- Those risks judged to be significant but with a lower level of likelihood should be detected as early as possible and monitored on a regular basis by RMC and Department Heads.

- Those risks judged to be insignificant, but with a high likelihood of occurrence should also be monitored closely by RMC and Department Heads.

- Risks judged to be insignificant with a low level of occurrence would likely not demand close attention.

- All staff should actively participate in identifying potential risks in their areas, and contribute to the implementation of appropriate remedial actions.

8. Assessing Risk Appetite

The level of risk that is acceptable, "the OAG's *'Risk Appetite'*" will be determined by the Auditor General who, in turn, is advised by RMC. Risk appetite may vary on a case by case basis depending on the issues being considered.

9. Exceptions to the Policy

There will not be any exception to the policy. It is applicable to the whole staff of the OAG.

10. Communication

- This policy is to be made available to all OAG staff, observed by all members of staff, both professional auditors and support staff.

- There will be an ongoing professional development and educational strategy to accompany the implementation of this policy.

- Risk Management policy will be integrated into the regular OAG's annual report.

11. Risk Register

The OAG should establish risk register whereby the assessment of risk of the Office is maintained.

12. Policy Implementation

Comprehensive management of risk in OAG involves absence of Office of the Auditor General audit Legislation, non-compliance of Code of Ethics, lack of independence, loss of trained qualified employees, political and technological changes and physical damage to OAG property.

12.1 Compliance with standards

The Office of the Auditor General of the State of Eritrea should consider compliance with the INTOSAI/ISSAI auditing standards in all matters that are deemed material in discharging its duties and responsibilities.

12.2 Office of the Auditor General's Audit Legislation

In order to fulfill its mission, The Office of the Auditor General must be governed by a legal framework (an audit Legislation).

12.3 Code of Ethics

The OAG and its personnel should adhere to the Code of Ethics especially relating to the principles of integrity, independence and objectivity, professional competence, conflict of interest, due professional care and professional secrecy.

12.3.1 Integrity

The OAG and its personnel should adhere to high standards of behaviour (e.g. honesty and candidness) in the course of their work and in their relationships with the staff of audited entities. Management must continually demonstrate, through words and actions, a commitment to high ethical standards.

12.3.2 Independence and objectivity

- The Auditor General and his/her Office must be impartial and accountable to the constitution and the law;

- The OAG and the Auditor must be independent from the audited entity and other outside interest groups.

- The OAG and the auditors must be independent from the audited entity and other outside interest groups.

- Auditors should be objective and impartial in dealing with the issues and topics under review.

12.3.3 Professional Competences

- The OAG must be staffed by personnel who maintain professional competence required to enable them to fulfill their responsibilities with due care.

- Auditors have a duty to conduct themselves in a professional manner at all times and to apply high professional standards in carrying out their work in order to enable them to perform their duties competently and with impartiality.

12.3.4 Conflict of interest

- The OAG should avoid conflict of interest between the auditor and the entity under audit.

- When auditors are permitted by the OAG to provide advice or services other than audit to an audited entity, care should be taken that these services do not lead to a conflict of interest.

12.3.5 Due professional care

The OAG and its personnel should exercise due care and concern in complying with the INTOSAI auditing standards. ISSAIs embrace due care in planning, specifying, gathering and evaluating evidence, and in reporting findings, conclusions and recommendations.

12.3.6 Confidentiality or professional secrecy

Auditors should not disclose information obtained in the auditing process to third parties.

13. Human resource policies and practices

The OAG should adopt policies and procedures to:-
- define knowledge and skills required for the position;

- establish, and regularly review, minimum educational requirements for the recruitment of personnel with suitable qualifications;

- recruit personnel with suitable qualifications;

- develop and train employees to enable them perform their tasks effectively;

- prepare manuals and other written guidance and instructions concerning the conduct of audits;

- support the skills and experience available within the Office and identify the skills which are absent;

- define responsibilities and tasks for the position, including clearly defined supervisory and reporting responsibilities.

13.1 Assignment of Duties and responsibilities

- The assignment of responsibility and the delegation of authority should be effected by clearly defined job descriptions, organizational charts depicting reporting responsibilities.
- Audit work should be assigned to personnel who have the degree of technical training and proficiency required in the circumstances.

- Annually Department Heads should review the responsibilities performed by their personnel and authorities granted and make changes where necessary.

13.2 Supervision and Review

- Establish the type of review of work that should be carried out at appropriate variance levels;

14. Political neutrality

The OAG and the auditors must be independent from political influence in order to discharge professional responsibilities in an impartial way.

15. Management's Philosophy and Operating Style (Tone at the Top)

The "tone at the top" (i.e. management's philosophy and operating style) should reflect a supportive attitude toward internal control at all times, independence, competence and leading by example which in turn are reflected in all aspects of management's actions. Thus management should:
- set a good example through its own actions and conduct;

- reflect what is proper rather than what is acceptable or expedient;

- set policies, procedures and practices that promote orderly, ethical, economical, efficient and effective conduct.

16. Review of Policy document

This risk document policy should be reviewed every two years.

17. Approval of Policy

This policy is approved by the Auditor General

Date: _____   Signature: _____

Definitions

Definitions are taken from the Australian & New Zealand Risk Management Standard.

Key definitions are:

Risk

The chance of something happening which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.

Consequence
The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Likelihood

A qualitative description or synonym for probability or frequency

Risk Assessment

The overall process of risk analysis and risk evaluation

Risk Management

The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects

Risk Treatment

Selection and implementation of appropriate options for dealing with risk conceptually, treatment options will involve one or a combination of the following five strategies;
- Avoid the risk
- Reduce the likelihood of occurrence
- Reduce the consequences of occurrence
- Transfer the risk
- Retain/Accept the risk.

Acknowledgment

This policy document has been prepared based on the following reference materials.

- AFROSAI-E Regularity Auditing
- INTOSAI 9130 Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management
- INTOSAI Code of Ethics and Auditing Standards.
- The International Standards for Supreme Audit Institutions (ISSAIs 30) Code of Ethics.
- COSO Enterprise Risk Management Integrated Framework.
- The Australian & New Zealand Risk Management Standard