Risk Management Policy

POL 31/2019
Version 3/2020

Commencement Date	20th December 2019 (Last Reviewed December 2020)
Relevant Legislation/ Reference Document	ISO 31000:2018 - Risk management Guidelines
Review Date	20th December 2022.

POLICY STATEMENT

1.0 Introduction

The purpose of the Risk Management Policy is to assist the Office of the Auditor General in integrating risk management into significant activities and functions. The effectiveness of risk management is dependent on its integration into the governance of the Office of the Auditor General which is inclusive of the decision-making process. The core requirement for a robust Risk Management Policy is the support from stakeholders, particularly Senior Executives and staff to understand and assist in incorporating risk management principles into daily activities. Everyone at OAG has the responsibility of managing risks through controls embedded into daily activities and decisions.

Effective and efficient management of risk plays a vital role in shaping the strategic focus. The criterion for successful and streamlined delivery of OAG's objective are outlines in the Audit Office's Business Plan 2020-2021. OAG's strategic focus is: - ***to provide independent and objective value adding services in conjunction with creating a working environment which allows for human capital to maximize potential.***

OAG is committed to achieving excellence in Public Sector Auditing and therefore have pledged commitment to adherence with International Standard on Risk Management, *ISO 31000: 2018 Risk Management Guidelines.*

To support the existence of a Risk Management Policy at OAG a resilient risk culture is essential. This is a reflection of the shared values, goals, practices and reinforcement mechanisms that embed risk into decision-making processes and risk management into its operating processes.

To maintain a robust risk management system the OAG is committed to ensuring:

- That risk management is an integral part of OAG planning and decision-making processes
- Consistency is maintained in risk management across OAG
- Roles, responsibilities and accountabilities are clearly articulated.

- Risk Management delegations are given appropriate discretion levels to undertake these responsibilities
- Risk Management delegations are supported with necessary skill sets to undertake these responsibilities
- Resources must be availed to achieve the stipulated policy outcomes
- Open communication is adopted and promoted for stakeholder engagement in identifying and management of risk

OAG will regularly review and monitor the implementation and effectiveness of the risk management process, including the development and embedding of an appropriate risk management culture across the organization.

OAG will strive in value creation and addition through continuously monitoring and adapting to the risk management framework to address external and internal changes.

OAG accepts that, in some instances, even with comprehensive risk management practices, adverse situations arise. In such situations, OAG will commit itself to review the reasons for the failure and endeavor to further strengthen controls to reduce the likelihood of a reoccurrence.

2.0 Scope

This Risk Management Policy applies to the following areas of the operations:

- Strategic, Operational and Business Planning processes, including Policy Development and Project Management
- Asset Management and Resource Planning
- Management of Ethics, Fraud and Security
- Business Interruption and Continuity Management
- Management of significant change issues e.g. organizational and technological changes
- Public Risk and General Liability Risks
- Workplace Health and Safety Risks
- Procurement and Contract Management
- Financial Management
- Human Resource Management

3.0 Objective(s)

The objective of this policy is to develop and implement an integrated strategy to guide OAG through managing its risks. This policy sets out procedures and communicates its commitment towards risk management:

- By integrating the management of risk across key functions and areas of responsibility
- By formalizing and enhancing existing risk management practices within the Office
- By demonstrating compliance with relevant legislation and regulatory requirements
- By raising the profile of risk management at all levels.
- By reducing the cost of risk, including injury, damage and loss to the office
- By developing and retaining a risk management plan and/or risk register to facilitate the

improved management of the risks

- By promoting good Corporate Governance
- By improving confidence and trust in the internal and external stakeholders through open communication.
- By ensuring a proactive approach to risk management
- By assisting in ensuring the Office's financial sustainability

4.0 Policy Maker(s) and Management

Policy Maker	Auditor-General
Management	Approval of Executive Management Committee

5.0 Keywords

Risk

Risk Management Process

Mitigation

6.0 Legislative framework

The legislative environment to be considered, and used for reference and guidance in implementing this policy are:

- Constitution of the Republic of Fiji 2013
- General Orders 2011
- Terms and Conditions of Employment for Government Wage Earners 2010
- Employment Relations Act and Regulations 2007
- Health and Safety at Work Act 1996
- Natural Disaster Management Act 1998
- Financial Management Act 2004 and Financial Instructions 2010, as amended
- Procurement Regulations 2010
- The OAG OHS policy

7.0 Supporting Procedures and Guidelines

This information will provide the background to the development of the policy should officers need clarification.

RESPONSIBILITIES	
Implementation	The Risk and Compliance Officer is responsible for implementing the policy.
Compliance	All Staff are responsible for complying with the policy.
Monitoring and Evaluation	The Risk and Compliance Unit is responsible for monitoring and evaluating the policy.
Implementation & Monitoring Designation	The Assistant Auditors General and Deputy Auditor General are responsible for implementation and monitoring of adherence with the framework
Development and/or Review	The Risk and Compliance Officer will be responsible for developing and/or reviewing the policy.
Interpretation and Advice	The Deputy Auditor-General is responsible for interpreting and advice on the policy.

8.0 Acronyms and Definitions

IIA
Institute of Internal Auditors

IoD
Institute of Directors

IRM
Institute of Risk Management

EMC
Executive Management Committee

Consequences

Outcome of an event affecting objectives

- A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives
- Any consequence can be expressed qualitatively or quantitatively
- Any consequence can escalate through cascading and cumulative effect.

Internal control

Internal controls are the mechanisms, rules, and procedures implemented by organizations' to ensure the integrity of financial and accounting information, promote accountability and prevent fraud. Besides complying with laws and regulations, and preventing employees from stealing assets or committing fraud, internal controls can help improve operational efficiency by improving the accuracy and timeliness of financial reporting.

Risk

Effect of uncertainty on objectives

- An effect of deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
- Objectives can have different aspects and categories, and can be applied at different levels.

Risk Management

Coordinated activities to direct and control an organisation with regard to risk

Stakeholder

Person or organisation that can affect, be affected or perceive themselves to be affected by a decision or activity

Risk Source

Element which alone or in combination has potential to give rise to risk

Event

Occurrence or change of a particular set of circumstances

- An event can have one or more occurrences, and can have several causes and several consequences
- An event can also be something that is expected which does not happen, or something that is not expected which does happen

Consequences

Outcome of an event affecting objectives

- A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives
- Any consequence can be expressed qualitatively or quantitatively
- Any consequence can escalate through cascading and cumulative effect.

Likelihood

Chance of something happening

- Refers to the chance of something happening whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as probability or frequency over a given time period.

Control

Measure that maintains and or modifies risk.

- Controls include but are not limited to any process, policy, device, practice or other conditions and or actions which maintain and or modify risk
- May not always exert the intended or assumed modifying effect.

Risk Analysis

Risk Analysis is to identify risks and document the risks to be managed. The aim is to identify the likelihood of something happening that can prevent the organization from achieving its goals and objectives.

Risk Acceptance

An informed decision to accept the consequences and the likelihood of a particular risk.

Risk Appetite

The amount of risk an organization is willing to accept or retain in order to achieve its objectives. Risk appetite = the organization's attitude towards risk taking.

Risk Assessment

The process of risk identification, risk analysis and risk evaluation.

Risk Criteria

Terms of reference against which the significance of a risk is evaluated.

Risk Control

The implementation of policies, protocols, standards, procedure and changes to eliminate or minimize adverse risks.

Risk Management

Coordinated activities to direct and control an organization with regard to risk.

Risk Management Policy and its links to Corporate Governance

The set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

Risk Management Plan

Is a document that is prepared to foresee risks, estimate impacts, and define responses to risks. It also contains a risk assessment matrix. A risk is "an uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives.

Risk Assessment Matrix

Is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase visibility of risks and assist management decision making

Risk Oversight

The Auditor General, Deputy Auditor General and Assistant Auditors General must proactively oversee, review and approve the approach to risk management regularly or with any significant business changes and satisfy itself that the approach is functioning effectively. Strategy and risk are inseparable and should permeate all organisational decisions and as such top management should consider a range of plausible outcomes that could result from its decision making and actions needed to manage those outcomes.

Risk Profile

A description of any set of risks. They can contain risks that relate to the whole organization, or part of the organization.

Risk Treatment

The selection and implementation of appropriate options for dealing with risk.

Risk Tolerance

The specific level of risk taking that is acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance = the practical application of risk appetite. For example, a risk appetite and risk tolerance organizational 'statement' provides officers with an understanding of acceptable risk levels. In cases where risk appetite is low, it provides guidance to officers on what decisions they cannot make. Where the organization is prepared to take increased levels of risk, this statement empowers officers to make appropriate risk-based decisions within certain parameters.

Shared risk

A risk with no single owner, where more than one organization is exposed or can significantly influence the risk

9.0 Compositions of the Office of the Auditor General's risk management Policy

9.1 The Risk Management Policy

The OAG risk management Policy is developed in line with ISSAI P12's objective focusing on the extent to which a SAI is able to make a difference to the lives of its citizens not only by strengthening the accountability, transparency and integrity of government and public sector entities through its audits; but also, by:

i. demonstrating ongoing relevance to citizens, Parliament and other stakeholders, and
ii. being a model organization through leading by example.

A SAI leads by example by ensuring good governance. Principle 9 of ISSAI P12 expects the SAI to assess organisational risk on a regular basis and supplement this with appropriately implemented and regularly monitored risk management initiatives.

In demonstrating ongoing relevance, Principle 5 requires SAIs to be responsive to changing environment and emerging risks by developing their work program to address the key issues affecting society, and ensuring that stakeholders' expectations and emerging risks are factored into strategic business and audit plans.
In providing independent and professional audit and assurance services to the Fijian Government Public Sector, Fijian Local Government, Statutory bodies and Provincial Councils, reputational damage is the most critical consequence should our risk management significantly fail. This document communicates the Audit Office's approach to risk management, which includes:

- articulating our risk management policy
- defining our risk appetite and risk tolerances
- developing a positive risk culture where risks are discussed regularly and either accepted or actively managed
- outlining key accountabilities and responsibilities
- stating our risk management methodology in identifying, assessing and monitoring strategic and operational risks.

9.2 Risk Appetite statement and tolerances

OAG's risk appetite is the amount of risk it is prepared to accept to achieve its strategic objectives. Having a documented risk appetite statement:

- allows for a better understanding of our strategic goals, culture, context and sensitivity to risk
- identifies different risk in across the organisation
- informs the development of risk tolerances for various OAG activities and decisions.

The risks to OAG can be significant and a failure to properly manage these risks will impact its ability to deliver its strategic objectives.

Risk tolerances are the boundaries for risk taking. The risk appetite statement informs the development of risk tolerances for OAG and provides guidance on how the risk appetite statement is to be applied in everyday business activities and decisions.

Refer to the risk register where the determined risk tolerances are captured for each risk.

The following table provides guidance for the relationship between risk appetite, risk tolerance and the adequate risk management approach.

Risk Score	Risk Level	Acceptability of Risk	Recommended Actions	Risk Owner
1-2	Low	Acceptable	Risk managed by routine controls and reviewed annually or after significant change No additional risk control measures required. Continue to monitor the risk does not escalate to higher level	All Staff and Contractors
3	Medium	Moderately Acceptable	Risk managed by an established, tailored control regime and reported quarterly to ECM. Acceptable to carry out work activity; however, tasks need to be reviewed to bring risk level to as low as reasonably achievable. Control measures must be implemented to reduce the risk. Supervisory oversight is required. Reviewed quarterly with intention to reduce the risk to low rating.	Assistant Auditors General and DAG
4	High	Moderately Acceptable	Risk is managed by an established, tailored controls regime which requires appropriate responsibility at senior level. Acceptable to carry out work activity; however, tasks need to be reviewed to bring risk level to as low as reasonably achievable Control measures must be implemented to reduce the risk. Reviewed monthly with intention to reduce the risk to low rating.	DAG
5	Extreme	Not Acceptable	Unacceptable level of risk and activity should stop immediately while mitigating plan is developed. Requires immediate escalation to AG and ECM. A mitigation plan owner on control effectiveness and mitigation plan/s. Control measures must be implemented to reduce the risk. Controls measures must focus on management and internal controls. Review at least once monthly.	AG

9.3 Risk Culture

Organisational culture refers to a set of shared values, behaviours, norms, beliefs and practices that characterize the functioning of a particular organisation. Risk culture refers to the set of shared values and behaviours that characterize how an entity considers risk in its day-to-day activities. However, the risk culture should be embedded into and not separate from the organizational culture.

Risk culture is the link that binds all the elements of risk management together, because it reflects the shared values, goals, practices and mechanisms that embed risk into an organization's decision-making processes and risk management into its operating processes.

The correlation of personal, organizational and risk culture has been illustrated below. Personal attributes are the skeleton of the risk perspectives which influence personal ethical conduct and behavior which in turn influences alignment with organizational and risk culture.

At OAG creation of a positive risk culture is fostered, where risk management is seen as a positive attribute for decision-making rather than a corrective measure. Hence, staff must be encouraged to have a willingness to engage effectively with risk.

Figure 1.0: Risk Culture Correlation – sourced IRM Risk Culture Framework

10.0 OAG Risk Management Process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. This process is illustrated below.

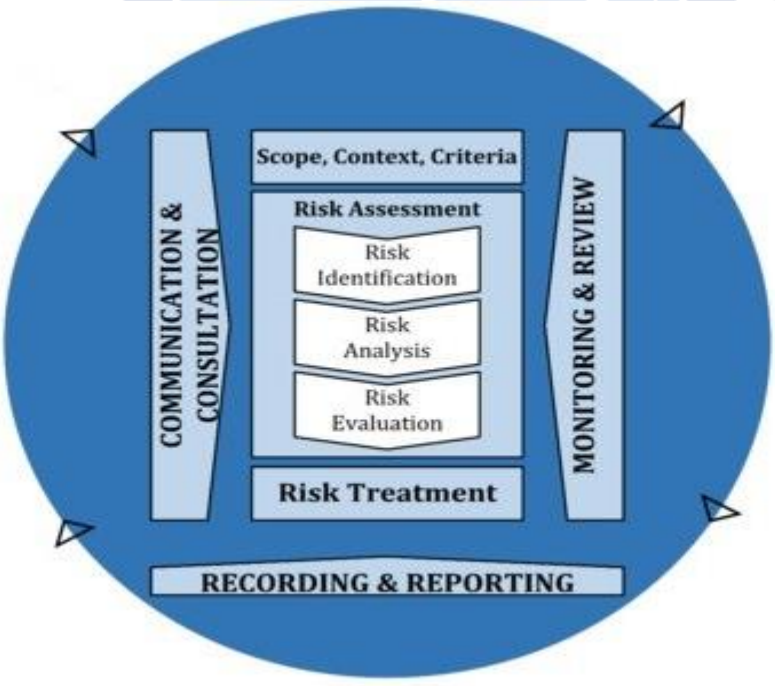

Figure 1.1: The Risk Management Process (based on ISO 31000: 2018 – Risk Management Guidelines)

The risk management process is an integral part of management and decision-making and integrated into the structure, operations and processes of the Audit Office. It can be applied at strategic, operational, programme or project levels.

The dynamic and variable nature of human behavior and culture are considered throughout the risk management process.

Although the risk management process is often presented as sequential, in practice it is iterative.

Risks shall be considered and assessed at different levels and across functions and activities of the OAG. All risk assessments and considerations shall be documented consistently using the OAG risk management process. All staff have a role in managing risk and are required to understand the business risks in their area and actively manage those risks as part of their day-to-day activities.

10.1 Communication and Consultation

At OAG the communication and consultation process assist relevant stakeholders both internal and external in understanding risk. The basis on which decisions are made and the reasoning behind a particular decision being made.

Communication serves as a mode to promote awareness and understanding of risk. On the contrary, consultation involves receiving feedback and information supporting the decision-making process. Synchronization of the two must facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into consideration confidentiality and integrity of information as well as the privacy rights of individuals.

Communication and consultation process at OAG with internal and external stakeholders should take place within and throughout all steps of the risk management process.

Communication and consultation at OAG aim to:

- bring different areas of expertise together for each step in the risk management framework;
- ensure that different views are appropriately considered when defining risk criteria and when evaluating risks;
- provide sufficient information to facilitate right oversight and decision making;
- build a sense of inclusiveness and ownership among those affected by risk

11.0 Scope, Context and Criteria

As the risk management process may be applied at different levels (e.g., strategic, operational, programme, project, or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organizational objectives.

11.1 External and internal context

The context of the risk management process should be established from the understanding of the external and internal environment of operations and should reflect the specific environment of the activity to which the risk management process is to be applied.

11.2 Defining risk criteria

OAG must specify the amount and type that it may or may not take, in correlation with the objectives.it must also define the criterion to evaluate the significance of risk and to support decision making processes Risk criteria should be aligned to the risk management framework and customized to the specific purpose and scope of the activity under consideration. It is a reflection of OAG's values, objectives and resources whilst being consistent with policies and statements.

Though the risk criteria were established on the onset this is subject to change based on the emerging risks, likelihood of risk occurrence, time band, standardization and organizational capacity.

11.3 Risk Assessment

OAG is committed to identifying and either eliminating or managing its risks. All Managers have a responsibility to involve their staff within this process. All areas of risk – for which risk assessments are to be conducted and documented – must be identified and listed in the risk register/risk management plan.

Hence, the office has established and will maintain a risk register/risk management plan where all identified risks are listed, together with details of actions taken. The register/plan will list all areas of risk that are yet to be addressed and they will be regularly assessed and updated. The risk areas will be prioritized and analyzed.

OAG requires that a formal risk assessment shall be undertaken in all the key areas of OAG, including when:

- planning and conducting audits
- developing corporate, group and unit business plans.
- assessing specific work health and safety implications or concerns
- conducting significant procurement activities
- undertaking business continuity and disaster recovery planning
- key business decisions

Staff should be aware of relevant tools to undertake risk assessments. These tools may include:

- The risk assessment process
- The risk register/risk management plan
- Relevant policies and guidelines

The risk assessment process will include the following steps:

- Identifying the risk to be assessed
- Establishing the staff committee groups.
- Identifying the risks and existing controls
- Undertaking the risk rating
- Identifying, if necessary, the additional controls/actions to be endorsed by management
- Allocating the appropriate actions/controls and scheduling review periods

- Reviewing/evaluating assessments
- Recording and Reporting

11.3.1 Risk Identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent OAG from achieving its objectives. Relevant, appropriate and current information is vital in the identification process.
All risks must be identified regardless of whether their sources are under control or not.

The major strategic risks which OAG is prone but not limited to are: Operational, Reputational, Procurement, Security, Infrastructure, Technological Risk together with Regulatory Compliance breaches and Change Management.

11.3.2 Risk Analysis

The purpose of risk analysis is to identify the nature of risk and its characteristics including, where appropriate, the level of risk. This involves detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness.

OAG uses risk analysis matrix to determine the level of risk. Risk rating of extreme, high, medium or low is determined and the likelihood of occurrence and implications of the event occurring are evaluated.
Both inherent and residual risk ratings are determined using the same assessment criteria.

Likelihood/Consequence	Rare	Unlikely	Possible	Likely	Almost certain
Insignificant	Low	Low	Low	Low	Medium
Minor	Low	Low	Medium	Medium	High
Moderate	Low	Medium	Medium	High	High
Major	Low	Medium	High	High	Extreme
Critical	Medium	High	High	Extreme	Extreme

Likelihood of occurrence
The likelihood of occurrence is determined through experience and probability of occurrence.

Likelihood of Risk	Definition	Probability
Rare	Possible but extremely unlikely	>90%
Unlikely	Possible but Unlikely	60-90%
Possible	Likely to happen	40-59%
Almost Certain	Almost certain; extremely likely	<10%

11.3.3 Risk Evaluation

The purpose of risk evaluation is to support decisions and are a build - up from the risk analysis. It involves comparison of the results derives from the risk analysis against established risk criterions here additional action is required. Decisions must take account of the wider context and the actual and perceived consequences to external and internal stakeholders. The result of the evaluation should be recorded, communicated and then validated at appropriate levels of the organisation.
Residual Risk Rating i.e., assessment of risk after implementing control measures is assessment against risk tolerance.

RISK APPETITE STATEMENT - Non-Comprisable

Number	Category / Subcategory	Principle Statement/s	Application of Principle Statement/s having regard to**
1	**Reputation**	Recognises that reputation is critical to our brand and has a **LOW**-risk appetite for risk in any of its activities that puts our reputation and ability to operate and or provide services in jeopardy; or could lead to loss of confidence by key stakeholders.	Reputation to be assessed in terms of our objectives as public sector auditors. Maintaining our international outlook as positive, growing and evolving with time and resources.
2	**Governance, Legal & Compliance**	Has a **LOW** tolerance for intentional and material breaches of Acts, laws, regulation, statutes, professional standards, Internal policies and Guidelines Has a **LOW** tolerance for criminal breaches, fraud and corruption, misuse of office or similar related activities.	A **LOW** risk tolerance for breach of our privacy obligations to staff and other stakeholders. Seeking opportunities to efficiently and effectively meet the requirements of internal policies and procedures.
		Has a **LOW** tolerance for risks relating to actions that may put critical functions and or operations in jeopardy.	
3	**OAG Values**	Has a **LOW** tolerance for intentional and material breaches of OAG Values and Code of Conduct. Has a **LOW** tolerance for unlawful discrimination based on gender, sexuality, ethnicity, culture, etc. Has a **LOW** tolerance for violence, sexual misconduct, harassment, bullying, and any other inappropriate behaviour and activities that puts our Culture of Respect in jeopardy.	Cultivate a cohesive and positive culture and an operating environment that is performance-based, customer-focused, entails ethical decision making and helps direct organisational effort, energy and resources towards the promotion, protection and overall success of OAG
4	**Health and Safety**	Aspires to **LOW** harm and is open to innovation and prudent investment in strategies to protect the health and wellbeing of our staff, contractors and visitors with a focus on the elimination and if not reasonably practicable to be eliminated, then minimisation of high-risk hazards.	Management supporting and leading a strong safety culture and expects employees to take personal responsibility for their own wellbeing.

5		Has **LOW** tolerance for safety management standards or practices that put the health and safety of our staff, contractors and visitors at risk.	
	Financial Sustainability	Has a **LOW**-risk appetite for pursuing any strategy that puts at risk the financial sustainability of the Audit Office over the medium to long term. Has a **LOW** appetite for application of capital that is not planned and executed in a sustainable and prudent manner.	A **MODERATE** appetite to increase revenue diversity
6	**Critical Operations**	Has a **LOW** tolerance for insufficient prevention and preparedness by management to avoid or minimise major disruptions to critical operations.	Has a **LOW** tolerance for significant operational disruptions to critical support/enabling operations and functions. Has a **HIGH** appetite for a comprehensive, coordinated and focused approach to effectively respond to and efficiently recover from disruptive incidents.

RISK APPETITE STATEMENT - Strategic

In addition to the above "non comprisable" statement the following statements provide guidance that will assist in making risk-based decisions

Number	Category / Subcategory	Principle Statement/s
7	**Organisational Culture**	Has a **HIGH** appetite to establish a collaborative, suitable, performance-focused, responsive and flexible culture that will enable organisational change to happen more readily and productively. Has a **HIGH** appetite to realise the benefits of diversity across gender, culture, ethnicity, etc. in the organisation.
8	**Research and Knowledge Transfer**	Subject to maintaining an exemplary quality and ethical standards, the Audit Office has a **HIGH** appetite to engage in research activities where there is a reasonable likelihood of achieving a positive outcome for our clients and OAG
9	**Partnerships**	Has a **MODERATE TO HIGH** appetite to leverage capacity and capability via internal and external partnerships, where this contributes to our strategic priorities.
10	**Workforce Capability**	Has a HIGH appetite to support strategies that build and sustain the appropriate culture, capabilities and resilience of our people.
11	**Systems and Information Management**	Recognises the critical need to protect and has a **LOW** risk tolerance for activities, events or behaviours that adversely impact on the confidentiality, integrity and availability of all critical business information.
12	**Asset Management**	Has a **LOW** tolerance for premises that do not meet applicable legal and regulatory compliance requirements. Has a **HIGH** appetite for optimal utilisation of assets and for their proper maintenance.

11.3.4 Rating of Existing Controls

The level of residual risk can be determined and compared with the predetermined risk tolerance to be able to decide if further treatment is needed.

Rating of Existing Controls

Controls Assessment		
Descriptor	**Foreseeable**	**Detail**
Inadequate	Less than what a reasonable person would be expected to do in the circumstances.	Little to no action being taken. No protection systems exist or they have not been reviewed for some time. No formalised procedures.
Adequate	Only what a reasonable person would be expected to do in the circumstances.	Being addressed reasonably. Protection systems are in place and procedures exist for common or typical circumstances. Periodic review.
Excellent	More than what a reasonable person would be expected to do in the circumstances.	Controls fully in place and require only ongoing maintenance and monitoring. Protection systems are being continuously reviewed and procedures are regularly tested.

12.0 Risk Treatment

The purpose of risk treatment is to select and implement options for addressing risk. This is an iterative process. Risk treatment selection options are formulated, implemented and evaluated taking into consideration its appropriateness. This is a balancing act between potential benefits to be derived relative to the achievement of the objectives against cost, effort or shortcomings of implementation.

It is noted that the risk treatment options are not necessarily mutually exclusive or applicable in all circumstances.

Stakeholder management is crucial in the process and appropriate communication and consultation methodologies must be devised to be able to achieve an agreeable risk management option.

A documented treatment plan should be integrated into the management plans and processes of the Audit Office in consultation with the stakeholders. The plan is to be articulate and concise as far as implementation is concerned.

13.0 Monitoring and Review

The purpose of the monitoring and review process is to ensure and improve the quality and effectiveness of the process design, implementation and outcomes. Continuous monitoring and periodic reviews of the risk management process and its outcome should be a planned part of the risk management process, with responsibilities clearly stated.

The monitoring and review process is applicable to all stages of the process and is inclusive of planning, gathering and analyzing information, recording of results and providing feedback.

Results derived from the monitoring and review process should be incorporated throughout the OAG's performance management, measurement and reporting activities.

This policy will be reviewed 12 months after implementation and every 3 years after that.

A bi – annual risk management status report will be submitted to Executive Management Committee. The Risk Management Plan to be reviewed annually and recommend any changes to the Executive Management Committee.

Additional reviews may occur through particular incidents, new technology, legislation/regulation changes and variations in resourcing. All reviews will take into account hazard and incident reports, and any other relevant information affecting the risk.

14.0 Recording and Reporting

The Risk Management Process and its outcomes must be documented and reported through appropriate mechanisms inclusive of but not limited to the risk assessment checklists, risk register, risk assessment report and presentations.

This will be actioned through submission to Executive Management Committee meeting on a quarterly basis by the Risk & Compliance Officer.
Furthermore, effective communication modes such as interpersonal, interpretive and presentational; will be selected to convey risk management activities and outcomes across the organization.

The Risk Management Plan to be reviewed annually and recommend any changes to the Executive Management Committee.

This policy will be reviewed 12 months after implementation and every 3 years after that.

Additional reviews may occur through particular incidents, new technology, legislation/regulation changes and variations in resourcing. All reviews will take into account hazard and incident reports, and any other relevant information affecting the risk.

15.0 Roles and Responsibilities

Governance of Risk: Three Lines of Defence Model
Internal audit has a key role in the corporate governance structure to assure on the effective management of risk:

The Executive Management Committee provides direction to senior management by setting the organisation’s risk appetite. It also seeks to identify the principal risks facing the organisation. Thereafter, the board assures itself on an ongoing basis that senior management is responding appropriately to these risks.

The Executive Management Committee delegates to senior management primary ownership and responsibility for operating risk management and control. It is management’s job to provide leadership and direction to the employees in respect of risk management, and to control the organisation’s overall risk-taking. The IIA and the IoD endorse the 'Three Lines of Defence model as a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided:

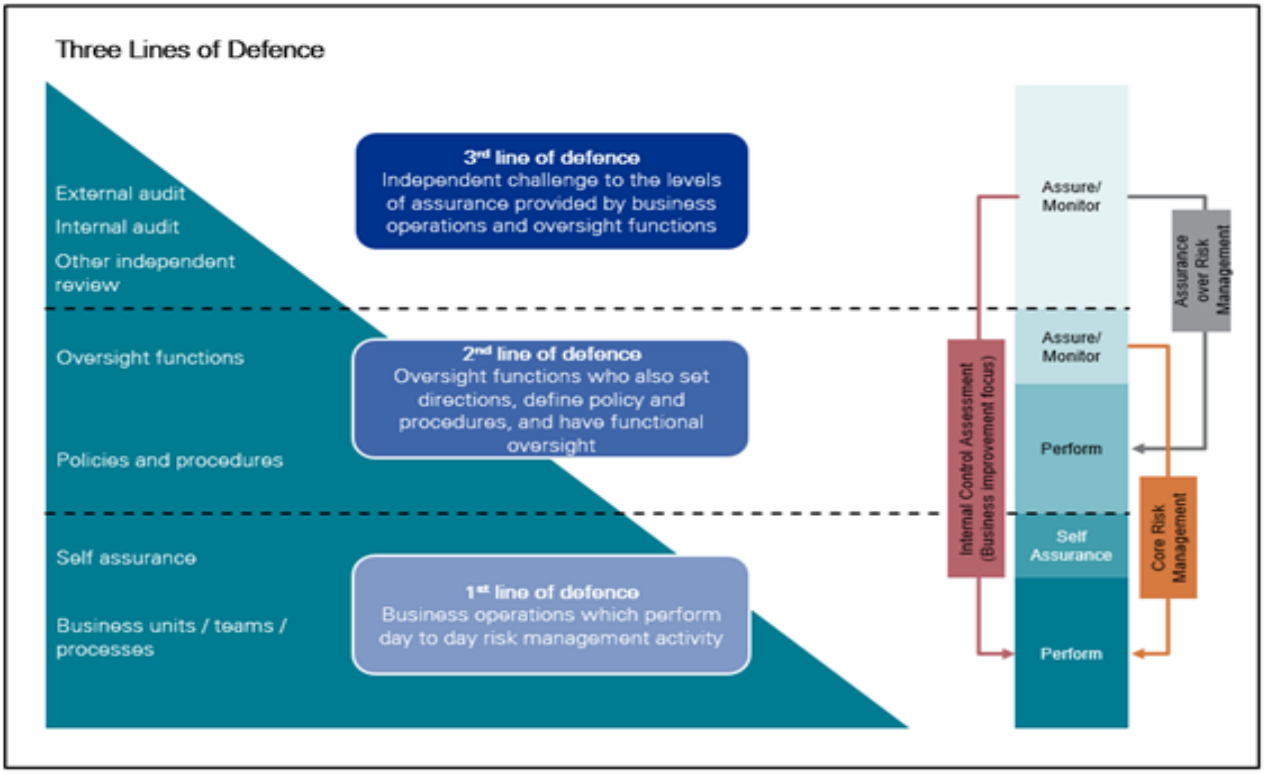

Figure 1.2: Three Lines of Defence functional representation Source -IIA

1. First line of defence

Under the first line of defence, operational management (Head of IT, Finance, People Management and Operations and Managers) has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.

2. Second line of defence

The second line of defence consists of activities covered by several components of internal governance (compliance, risk management, quality, IT and other control departments). This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk related information up and down the organisation.

3. Third line of defence

Internal audit forms the organisation's third line of defence. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organisation's board of directors and senior management.

This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence. It encompasses all elements of an institution's risk management framework (from risk identification, risk assessment and response, to communication of risk related information) and all categories of organisational objectives: strategic, ethical, operational, reporting and compliance.

15.1 Roles and Responsibilities of Executive Management

To ensure the effectiveness of OAG's risk management Policy, the Executive Management need to be able to rely on adequate line functions – including monitoring and assurance functions – within the OAG.

The key responsibilities of Executive Management towards risk management are detailed as follows:

The Deputy Auditor General

The Deputy Auditor General is responsible for overseeing that a Risk Management Plan is established, implemented and maintained in accordance with this policy, and for the assignment of responsibilities in relation to risk management.

Management, Department Heads & Risk & Compliance Officer

The OAG Management Team – Assistant Auditor's General, Audit Managers & Risk and Compliance Officer are responsible for the implementation of the Office's Risk Management Plan within their respective areas of responsibility.

This includes the identification, assessment, recording and reviewing of risks, establishment of controls through systems and processes, and the assignment and completion of risk control actions.

The Risk and Compliance Officer are responsible for facilitating and resourcing to enable compliance with the Risk Management Plan.

The Deputy Auditor General, Head of IT, Finance, People Management and Operations, Assistant Auditor's General, Audit Managers and Senior Officers for the measurement of performance of staff against the strategic priorities in the Office's Strategic Plan, Operational Plan and the Key Performance Indicators in team and individual officer's work plans.

The monitoring of all risks and regular reviews of the risk management plan and/or register will be managed by Risk and Compliance Officer.

All Staff

Effective risk management depends on the commitment and co-operation of all staff. All staff have a significant role in the management of risk, particularly within their own areas of control.

All staff have responsibilities for managing the risks in their activities and workplace, and are accountable through their individual work plans. Staff will report to their Managers on the status of the implementation of their respective aspects of the Risk Management Plan at their regular team meetings, and will refer issues to Risk and Compliance Officer under guidance of Deputy Auditor General when additional resourcing is required. Staff roles include:

- Identifying risks related to the achievement of their team's operational/business plan and to advise their managers of the risks.
- Identify relevant mitigation actions and to include these within their team's Individual Work Plan, and to ensure to the best of their ability that the team's work plan is met.
- To be aware of other risks that may develop during the year
- To provide feedback for updating the risk register/risk management plan and to proactively discuss new inputs during regular team meetings

16.0 Who to Contact About this Policy

Any queries are directed to Deputy Auditor-General.

17.0 Approval

The Risk Management Policy becomes effective on the date approved by the Executive Management Committee.

18.0 Revision/Change Log

Version 3.0	
Policy endorsed by:	Executive Management Committee
Policy reviewed by PDRC:	4th November 2020
Policy effective from:	25th February 2021
Policy to be reviewed by:	20th December 2022
Manager responsible for policy:	Head of IT, Finance, People Management and Operations

Version 2.0	
Policy endorsed by:	Executive Management Committee
Policy approved by:	Auditor-General
Policy reviewed by PDRC:	06 December 2019
Policy effective from:	20th December 2019
Policy to be reviewed by:	20th December 2020
Manager responsible for policy:	Head of IT, Finance, People Management and Operations

Version 1.0	
Policy endorsed by:	Executive Management Committee
Policy approved by:	Auditor-General
Policy effective from:	24th January 2019
Policy to be reviewed by:	24th January 2020
Manager responsible for policy:	Manager Corporate Services