OAG Best Practice Guide: Risk Management

OFFICE of the AUDITOR GENERAL
Republic of Fiji

Customer Advisory Services
July 2020

BEST PRACTICE GUIDES

The Office of the Auditor General (OAG) significantly contributes to the functioning of public services and public accountability. The Office has embarked on expanding its role through advisory activities to reinforce its audit work. One such activity involves producing best practice guides that can be widely used in the Fiji public sector.

Through the introduction of best practice guides, we have endeavoured to ensure the best impact possible on public policies and their implementation. In doing so, the OAG is focused on improving processes in the public sector, in order to enhance the economy and efficiency of public administration and improve public operational governance.

This is also an endeavour by the OAG to align itself to the *ISSAI*[1] *12: Value and Benefits of SAIs,* which conveys that the ultimate role of a supreme audit institution is to have impact, and to make a difference in the lives of citizens. In line with this standard, our ultimate objective is better visibility of the value and benefits of our work for our audited entities, for decision-makers in Parliament, Government and administrations, as well as our citizens.

DISCLAIMER

This best practice guide has been compiled for reference only and is not intended to represent the best or only approach to risk management or any particular issue. We have done our best to ensure that the publications and other information in this guide are up to date, however some information in a publication will inevitably lose relevance or currency over time.

One should not treat information in this guide as amounting to definitive professional advice about any specific matter. Users should seek appropriate accounting, legal or other professional advice to address specific facts and circumstances. The OAG does not accept legal responsibility for reliance on information in this guide.

Members or officials of public office should utilize this guide in light of their professional judgment, and the facts and circumstances involved in their public office and each particular engagement or situation. The OAG disclaims any responsibility or liability that may occur, directly or indirectly, as a consequence of the use and application of this guide.

[1] International Standards of Supreme Audit Institutions

GLOSSARY

Consequences Outcomes 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; and can escalate through a cascading and a cumulative effect.

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; and may not always exert the intended or assumed modifying effect.

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. It can also be something that is expected but which does not happen, or something that is not expected but which does happen.

Internal control The mechanisms, rules, and procedures implemented by organisations 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. (Kenton, 2019)

Likelihood Chance of something happening whether defined, measured or determined objectively, subjectively, qualitatively or quantitatively and described using general terms or mathematically (using probability or frequency over a given time period).

Risk The effect of uncertainty on objectives. This effect of deviation from the expected, 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 Acceptance An informed decision to accept the consequences and the likelihood of a particular risk.

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

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

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

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

Risk Management Coordinated activities to direct and control an organisation with regard to risk.

Risk Management Framework 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 Oversight The Permanent Secretary, Deputy Permanent Secretary and Head of the Department/*(Head of the Organisation and Executive Management)* 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 Management Plan A document that is prepared to foresee risks, estimate impacts, and define responses to risks. It also contains a risk assessment matrix.

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

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 is 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. (Deakin University, 2019)

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

Stakeholder A person or an organisation that can affect, be affected or perceive themselves to be affected by a decision or activity.

ACRONYMS

IIA	Institute of Internal Auditors
IoD	Institute of Directors

CONTENTS

Best Practice Guides 1

Disclaimer 1

Glossary 2

Introduction 5

1.0 Scope 5

2.0 Objective 6

3.0 Legislative Framework 6

4.0 Composition of the Risk Management Framework 6

4.1 The Risk Management Policy 6

4.2 Risk Appetite Statement and Tolerance 7

4.3 Risk Culture 8

5.0 Risk Management Process 8

5.1 Communication and Consultation 9

5.2 Scope, Context and Criteria 9

5.2.1 External and internal context 10

5.2.2 Defining risk criteria 10

5.3 Risk Assessment 10

5.3.1 Risk Identification 11

5.3.2 Risk Analysis 11

5.3.3 Risk Evaluation 11

5.4 Risk Treatment 11

5.5 Monitoring and Review 12

5.6 Recording and Reporting 12

6.0 Roles and Responsibilities 13

6.1 Governance of Risk: Three Lines of Defence Model 13

6.1.1 First Line of Defence 13

6.1.2 Second Line of Defence 14

6.1.3 Third Line of Defence 14

6.2 Roles and Responsibilities of Executive Management 14

6.2.1 The Head of the Organisation 14

6.2.2 Management, Department Heads & Risk & Compliance Officer 14

6.3 Roles and Responsibilities of Staff 14

6.4 Who to Contact About the Risk Management Guideline/Policy 15

6.5 Supporting Procedures and Guidelines 15

6.6 Approval 15

7.0 Conclusion 15

References 16

INTRODUCTION

This Best Practice Guide aims to assist organisations in the emerging critical area of Risk Management. Developing a guidance and/or policy would ideally have its main objective to assist the organisation in integrating risk management into significant activities and functions. The effectiveness of risk management is dependent on its integration into the governance of the organization which is inclusive of the decision-making process. The core requirement for any Risk Management Guidance/Policy is the support from stakeholders, particularly Senior Executives and staff to understand and assist in incorporating risk management principles into daily activities. Everyone in the organisation 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 the organisation's objectives are outlined in the Operational Plan. The organisation's strategic focus should also be stated here. It would be ideal for organisations in the public sector to consider adherence with the International Standard on Risk Management, *ISO 31000: 2018 Risk Management Guidelines.*

To support the existence of a Risk Management guide and/or policy in any organisation, 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 an organisation ought to be committed to ensuring:

- Risk management is an integral part of (organisational) planning and decision-making processes
- Consistency is maintained in risk management across the (organisation)
- 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 are made available to achieve the policy outcomes
- Open communication is adopted and promoted for stakeholder engagement in identifying and management of risk

It is advisable for organisations to 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. Value creation and addition can also be achieved through continuous monitoring and adapting to the risk management framework, to address external and internal changes. In some instances, even with comprehensive risk management practices, adverse situations will arise. In such situations, the ideal solution would be for the organisation to commit itself to review the reasons for the failure, and endeavor to further strengthen controls to reduce the likelihood of a reoccurrence.

1.0 SCOPE

The developing of a Risk Management guide and/or policy would ideally apply to the following areas of 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

2.0 OBJECTIVE

The objective of a Risk Management guide and/or policy would be to develop and implement an integrated strategy to guide the organisation through managing its risks. Any such guide and/or policy may set out procedures and communicate its commitment towards risk management by:

- Integrating the management of risk across key functions and areas of responsibility
- Formalising and enhancing existing risk management practices within the organisation
- Demonstrating compliance with relevant legislation and regulatory requirements
- Raising the profile of risk management at all levels.
- Reducing the cost of risk, including injury, damage and loss to the office
- Developing and retaining a risk management plan and/or risk register to facilitate the improved management of the risks
- Promoting good Corporate Governance
- Improving confidence and trust in internal and external stakeholders through open communication.
- Ensuring a proactive approach to risk management
- Assisting in ensuring the organisation's financial sustainability

3.0 LEGISLATIVE FRAMEWORK

The legislations that need to be considered for reference and guidance in implementing any Risk Management guide and/or policy in the public sector 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
- OHS Policy

4.0 COMPOSITION OF THE RISK MANAGEMENT FRAMEWORK

4.1 The Risk Management Policy

In providing quality and professional services to the general public, reputational damage is the most critical consequence when an organisation fails to manage its risks. It is ideal for a policy to communicate the following:

- The organisation's approach to risk management
- Defining 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 a risk management methodology in identifying, assessing and monitoring strategic and operational risks.

4.2 Risk Appetite Statement and Tolerance

The organisation's risk appetite is the amount of risk it is prepared to accept in order to achieve its strategic objectives. Having a documented risk appetite statement provides a better understanding of our strategic goals, culture, context and sensitivity to risk; a means of identifying different risks across the organisation; and a background on the development of risk tolerances for various organisational activities and decisions.

The risks to an organisation 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 states the development of risk tolerances for the organisation and provides guidance on how it is to be applied in everyday business activities and decisions.

The risk register documents the determined risk tolerances for each risk.

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

Table 1: Risk Appetite, Risk Tolerance, Adequate Risk Management Approach

Risk Score	Risk Level	Acceptability of Risk	Recommended Action	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 so it does not escalate to a higher level.	All Staff and Contractors
3-4	Medium	Moderately Acceptable	▪ Risk managed by an established, tailored control regime and reported quarterly to Executive Management. ▪ 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.	Assistant PS or Designated Office Holder/ Heads of Departments
4-5	High	Not Acceptable	▪ Unacceptable level of risk and activity should stop immediately while mitigating plan is developed. ▪ Requires immediate escalation to Executive Management. ▪ A mitigation plan owner on control effectiveness and mitigation plan/s. ▪ Control measures must be implemented to reduce the risk. ▪ Control measures must focus on management and internal controls.	The Head of the Organisation

4.3 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. (DeLoach, 2017)

The correlation of personal, organizational and risk culture is illustrated in Figure 1 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.

In the organisation 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.

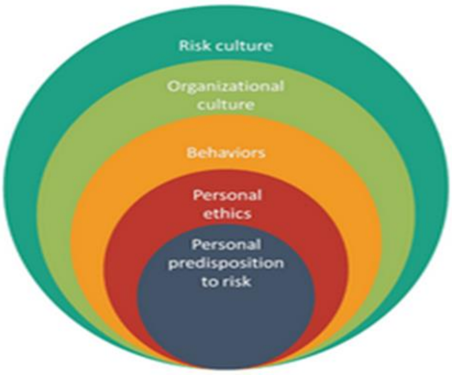


Figure 1: Risk Culture Correlation *(Source: Institute of Risk Management Risk Culture Framework)*

5.0 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 in Figure 2 below.

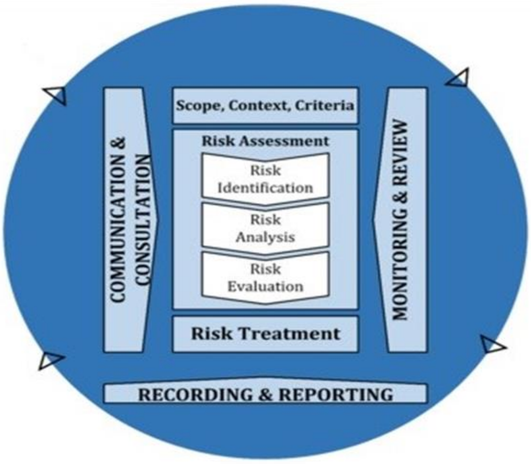


Figure 2: The Risk Management Process *(Based on ISO 31000: 2018 – Risk Management Guidelines)*

The risk management process is an integral part of management and decision-making and integrated into the structure, operations and processes of the ministry. It can be applied at the 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 ministry. All risk assessments and considerations shall be documented consistently using the 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.

5.1 Communication and Consultation

The communication and consultation process within the organisation 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, while 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 processes with internal and external stakeholders should take place throughout all steps of the risk management process. The objectives of this process are shown in Figure 3 below:

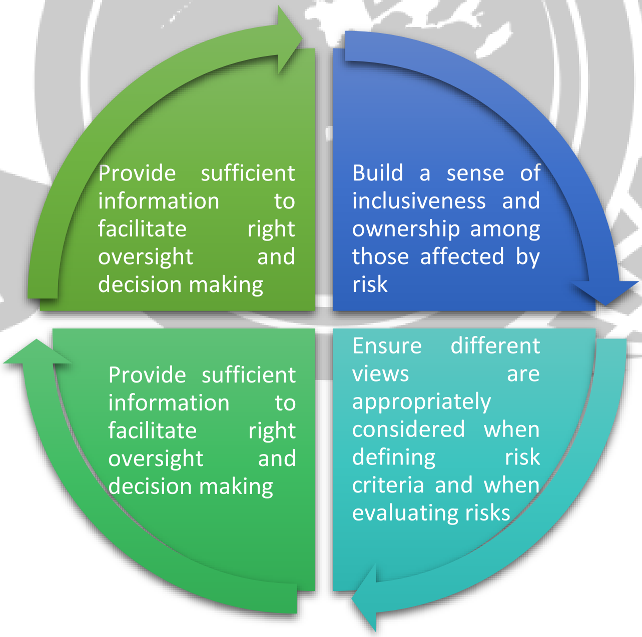

Provide sufficient information to facilitate right oversight and decision making
Build a sense of inclusiveness and ownership among those affected by risk
Provide sufficient information to facilitate right oversight and decision making
Ensure different views are appropriately considered when defining risk criteria and when evaluating risks

Figure 3: Objectives of Communication and Consultation in the Risk Management Process

5.2 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.

5.2.1 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.

5.2.2 Defining risk criteria

The organisation must specify the amount and type of risk 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 the ministry's values, objectives and resources whilst being consistent with policies and statements.

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

5.3 Risk Assessment

The organisation should be 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 organisation will establish and 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.

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

- planning and conducting any organizational activity;
- developing the 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; and
- making 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, and relevant policies and guidelines. The risk assessment process includes the following steps:

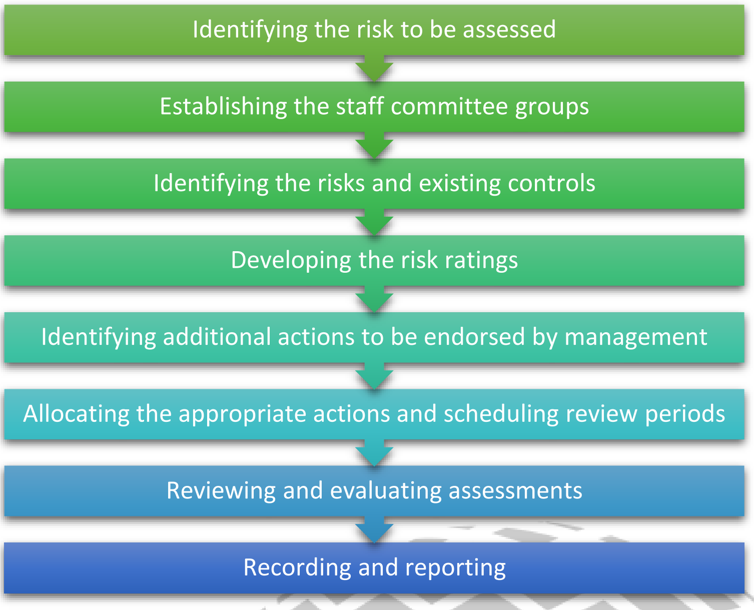

Identifying the risk to be assessed
Establishing the staff committee groups
Identifying the risks and existing controls
Developing the risk ratings
Identifying additional actions to be endorsed by management
Allocating the appropriate actions and scheduling review periods
Reviewing and evaluating assessments
Recording and reporting

Figure 4: The Risk Assessment Process

5.3.1 Risk Identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent the ministry 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 an organisation is prone to but not limited to are: Operational, Reputational, Procurement, Security, Infrastructure, Technological Risk together with Regulatory Compliance breaches and Change Management.

5.3.2 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.

5.3.3 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 derived from the risk analysis against established risk criteria where 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.

5.4 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.

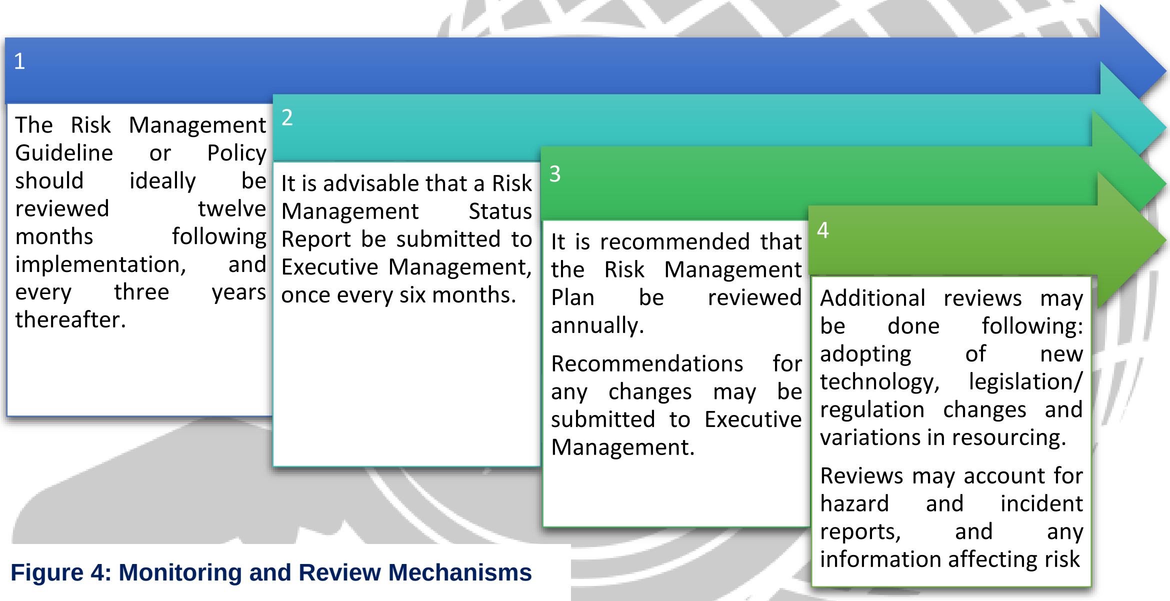
A documented treatment plan should be integrated into the management plans and processes of the ministry in consultation with the stakeholders. The plan is to be articulate and concise as far as implementation is concerned.

5.5 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 organisation's performance management, measurement and reporting activities. Mechanisms to assist in this phase of the process are shown in the following diagram:



1

The Risk Management Guideline or Policy should ideally be reviewed twelve months following implementation, and every three years thereafter.

2

It is advisable that a Risk Management Status Report be submitted to Executive Management, once every six months.

3

It is recommended that the Risk Management Plan be reviewed annually.

Recommendations for any changes may be submitted to Executive Management.

4

Additional reviews may be done following: adopting of new technology, legislation/ regulation changes and variations in resourcing.

Reviews may account for hazard and incident reports, and any information affecting risk

Figure 4: Monitoring and Review Mechanisms

5.6 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 meetings 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. (Brown, 2019)

6.0 ROLES AND RESPONSIBILITIES

6.1 Governance of Risk: Three Lines of Defence Model

The Three Lines of Defense model distinguishes among three groups (or lines) involved in effective risk management. These are firstly functions that own and manage risks; followed by functions that oversee risks; and finally functions that provide independent assurance. (IIA)

The Executive Management/Board 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 Executive Management/Board assures itself on an ongoing basis that senior management is responding appropriately to these risks. Internal audit also has a key role in the corporate governance structure to assure on the effective management of risk.

The Executive Management/Board delegates to senior management primary ownership and responsibility for operating risk management and control. It is senior management's responsibility to provide leadership and direction to employees in respect to 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.

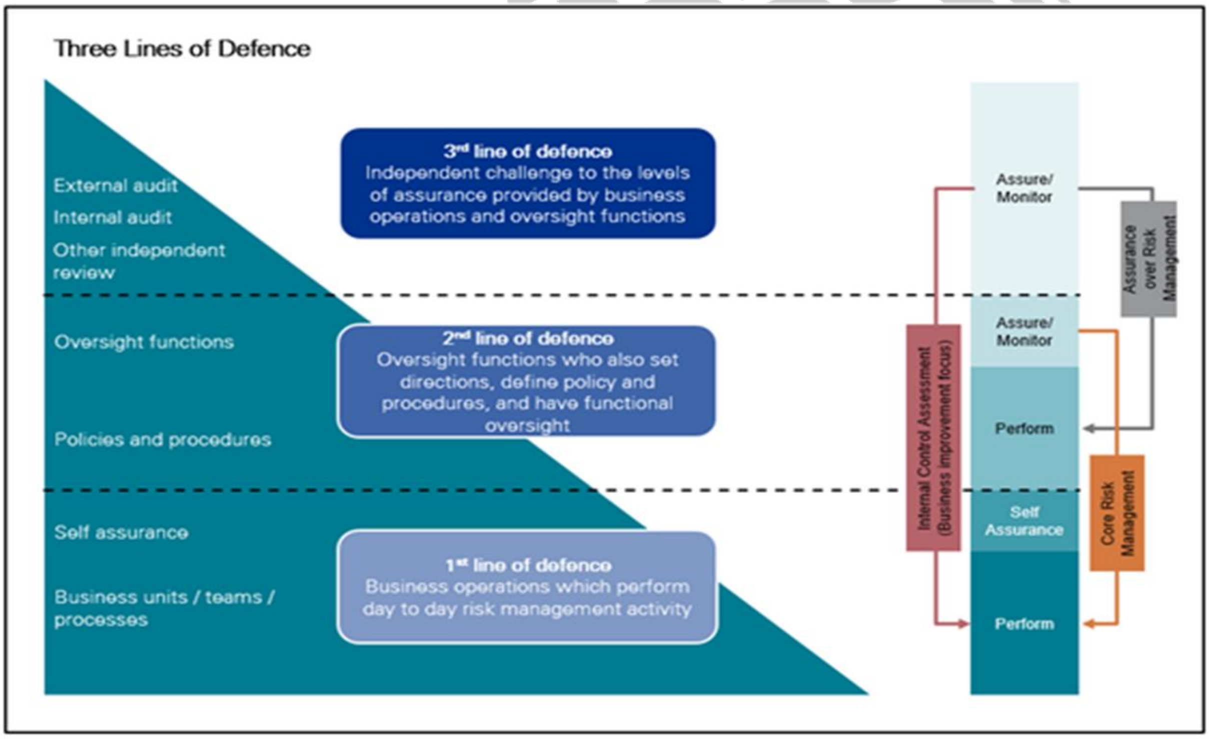

Three Lines of Defence
External audit
Internal audit
Other independent review
Oversight functions
Policies and procedures
Self assurance
Business units / teams / processes
3rd line of defence
Independent challenge to the levels of assurance provided by business operations and oversight functions
2nd line of defence
Oversight functions who also set directions, define policy and procedures, and have functional oversight
1st line of defence
Business operations which perform day to day risk management activity
Assure/ Monitor
Assure/ Monitor
Perform
Self Assurance
Perform
Internal Control Assessment (Business improvement focus)
Assurance over Risk Management
Core Risk Management

Figure 5: Three Lines of Defence *(Source – IIA)*

6.1.1 First Line of Defence

Operational management naturally serves as the first line of defense because controls are designed into systems and processes under their guidance of operational management. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events. (IIA)

Operational management (Directors, Head of Departments, and Managers) have ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.

6.1.2 *Second Line of Defence*

Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-defense controls.

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.

6.1.3 *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. (Chartered IIA)

6.2 Roles and Responsibilities of Executive Management

To ensure the effectiveness of an organization's risk management framework, the Executive Management needs to be able to rely on adequate line functions – including monitoring and assurance functions – within the organisation. The key responsibilities of Executive Management towards risk management are detailed as follows:

6.2.1 *The Head of the Organisation*

The Permanent Secretary/Chief Executive Officer 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.

6.2.2 *Management, Department Heads & Risk & Compliance Officer*

The Management Team – Directors, Head of Departments and Risk and Compliance Officer are responsible for the implementation of the organisation'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 is responsible for facilitating and resourcing to enable compliance with the Risk Management Plan.

The Permanent Secretary/Chief Executive Officer, Directors, Head of Departments and Senior Officers are responsible for the measurement of staff performance against the strategic priorities in the organisation's Strategic Plan, Operational Plan, and Key Performance Indicators in work plans at the team and individual levels.

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

6.3 Roles and Responsibilities of Staff

Effective risk management depends on the commitment and co-operation of all staff, who 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 the Risk and Compliance Officer under guidance of the Permanent Secretary/Chief Executive Officer, when additional resourcing is required. These roles are further illustrated below:

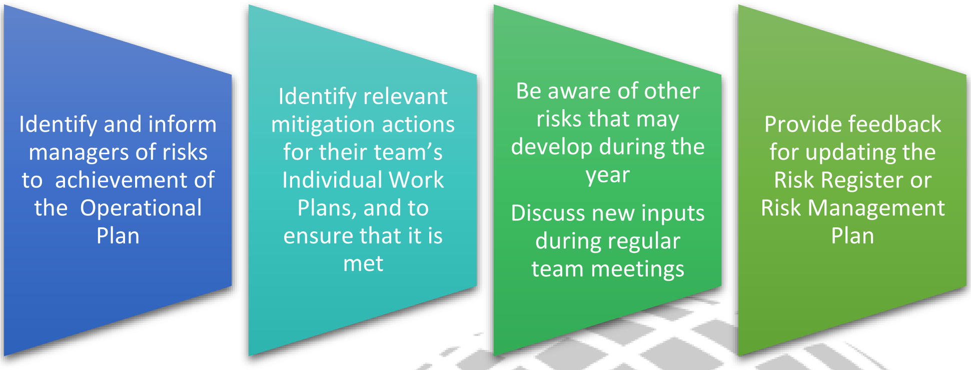

Identify and inform managers of risks to achievement of the Operational Plan
Identify relevant mitigation actions for their team's Individual Work Plans, and to ensure that it is met
Be aware of other risks that may develop during the year
Discuss new inputs during regular team meetings
Provide feedback for updating the Risk Register or Risk Management Plan

Figure 6: Roles of Staff in the Risk Management Process

6.4 Who to Contact About the Risk Management Guideline/Policy

Any queries would be directed to the Deputy Permanent Secretary/ *(designated office holder)*.

6.5 Supporting Procedures and Guidelines

Responsibility	Responsible Officer
Implementation	The *(designated office holder)* is responsible for implementing the guideline/policy
Compliance	All staff are responsible for complying with the guideline/policy
Monitoring and Evaluation	The *(designated office holder)* is responsible for monitoring and evaluating the guideline/ policy
Development and/or Review	The *(designated office holder)* is responsible for developing and/or reviewing the guideline/ policy
Interpretation and Advice	The *(designated office holder)* is responsible for interpreting and providing advice on the guideline/policy

6.6 Approval

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

7.0 CONCLUSION

The primary goal for any risk management framework or process is to cultivate a risk management culture, where employees and stakeholders are conscious of the importance of monitoring and managing risk. The anticipated benefits of an effective risk management framework for organisations in the public sector would be the identifying of opportunities and threats in a timely manner, the ability to respond effectively to change, and increasing stakeholder confidence and trust.

REFERENCES

Brown, J. (2019, March 30th). Security Solutions Media .

Retrieved from https://www.securitysolutionsmedia.com/2019/03/30/enterprise-risk-management/

Chartered Institute of Internal Auditors. (2019, October 7th).

Retrieved from https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

Deakin University. (2019, November 25th). Deakin University.

Retrieved from https://policy.deakin.edu.au/document/view-current.php?id=94

DeLoach, J. (2017, June 5th). Corporate Compliance Insight.

Retrieved from https://www.corporatecomplianceinsights.com/10-principles-for-effective-board-risk-oversight/

Kenton, W. (2019, June 25th). Investopedia.

Retrieved from https://www.investopedia.com/terms/i/internalcontrols.asp

Office of the Auditor General, Republic of Fiji . (n.d.).

OAG - Risk Management Policy. Suva : Office of the Auditor General, Republic of Fiji .

The Institute of Internal Auditors Global. (n.d.).

IIA POSITION PAPER. 247 Maitland Avenue, Altamonte Springs, Florida 32701 USA.