

MINISTRY OF FINANCE, ECONOMIC PLANNING AND DEVELOPMENT

Circular No 8 of 2021

Our Ref: CF/40/30/10/50/A

28 December 2021

From: Financial Secretary

To: Supervising Officers-in-Charge of Ministries/Departments and Accounting Officers

Guidelines for establishment of Risk Management in the Public Sector

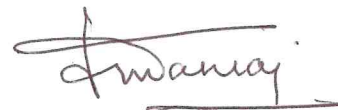
The purpose of this Circular is to inform you of the process for putting in place a Risk Management Framework (RMF) at the level of your Ministry/Department.

2. As you are aware, the Annex to the Budget Speech 2021/22 provides for the establishment of a formal risk management framework to support Ministries/Departments in setting out the overall architecture for the management and mitigation of risks.

3. Accordingly, in order to facilitate the process for the establishment of a Risk Management Framework in Ministries/Departments, this Ministry has developed the enclosed '*Guidelines for Risk Management in the Public Sector*' with appropriate templates and examples of risk categories.

4. Furthermore, a dedicated team at the Internal Control Cadre of this Ministry has been set up to provide support in developing your RMF. You may contact the Director, Internal Control for any assistance required.

5. You are kindly requested to ensure compliance with the content of this Circular.



**D. D. Manraj, GOSK
Financial Secretary**

Copy to:

- (i) *Secretary to Cabinet and Head of the Civil Service*
- (ii) *Director of Audit*
- (iii) *Director, Internal Control*



Guidelines for Risk Management in the Public Sector

Ministry of Finance, Economic Planning and Development

December 2021

Contents

Preface	2
Interpretation	3
Introduction	4
Risk Management Framework	5
Enterprise-wide risk Management (ERM)	6
Integration of Risk Management Activities	6
Structural Configuration of the Risk Management Framework	8
Risk Identification	8
Risk Assessment	9
Risk Response	11
Designing control activities to mitigate risks	11
Risk Monitoring.....	11
Communication and Reporting	12
Accountability, Roles and Responsibilities	12
Risk Management Functions of Ministries/Departments.....	12
Risk Management Functions of Accounting Officers	13
Evaluation of Risk Management Effectiveness	15
Anti-Money Laundering and Combatting the Financing of Terrorism .	17
Risk Categories	20

Preface

The annex to Budget Speech 2020/21 provides for the strengthening of internal audit and risk management in the Public Sector.

Risk management is a fundamental element of corporate governance. Risk is associated with possible events which, should they occur, could prevent a Ministry/Department from fulfilling its mission, meeting its commitments and achieving its objectives. Risks may adversely affect the Ministry/Department's strategy, people, assets, environment or reputation.

Effective risk management supports good governance as it assists in determining priorities and setting objectives, in analysing uncertainties within decision-making arrangements, in clarifying accountabilities and in demonstrating how the public interest is best served.

Accordingly, a set of guidelines has been developed for the establishment of formal risks management structures or processes in the public sector.

These guidelines will assist Accounting Officers to develop a **risk management framework** according to the specificities of Ministries/Departments and facilitate the following processes:

- (i) risk identification;
- (ii) risk assessment;
- (iii) risk response;
- (iv) designing control activities to mitigate risks;
- (v) risk monitoring; and
- (vi) risk communication and reporting.

The Internal Control Cadre and Audit Committees will assist Accounting Officers in establishing the risk management framework.

Interpretation

In this Framework,

“**Accounting Officer**” has the same meaning as in the Finance and Audit Act [Section 21(1)].

“**Audit Committee**” is an integral element of public accountability and governance and plays a key role in assisting Ministries/Departments in their legal and fiduciary responsibilities, especially with respect to the integrity of the Government’s financial information and the adequacy and effectiveness of the internal control system.

“**Inherent Risk**” is the exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.

“**Internal Auditing**” is, to objectively and systematically evaluate the effectiveness of risk management, control and governance processes, provide assurance on the efficient use and management of resources within the Ministry/Department. This function is carried out by the Internal Control Cadre

“**Residual Risk**” is the remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk).

“**Risk**” means an unwanted outcome, actual or potential, to the institution’s service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of “risk” also encompasses such opportunities.

“**Risk Appetite**” is the amount of residual risk that the Ministry/Department is willing to accept.

“**Risk Factor**” is any threat or event which create, or has the potential to create risk.

“**Risk Management**” is the systematic and formalised process to identify assesses, manage and monitor risks and the amount of risk that the Ministry/Department is capable of bearing (as opposed to the amount of risk it is willing to bear).

Introduction

Purpose

1. The purpose of this guidance is to update Ministries/Departments with current good practice, to support them with embedding risk management into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture.
2. The Framework aims to support Ministries/Departments in setting out the overall architecture within the organisation for the management and mitigation of risk. A comprehensive risk management process facilitates Ministries/Departments in achieving their business objectives and positions risk within the overall governance structures of the organisation.

Applicability

3. The Framework recognises that Ministries/Departments are not necessarily similar in the nature of their operations hence it is not possible to produce a one-size-fits-all approach to be replicated across Ministries/Departments. Therefore, this Framework adopts the approach of setting the general principles, standard, models and practices proven to support and sustain effective risk management. Ministries/Departments may adapt this framework and add any provisions to reflect their specificities. This Framework has been developed by taking into consideration the essence of '*ISO 31000-Risk Management*' and best international practices.

Risk Management Framework

4. A risk management framework is an integral part of the Ministry/Department's planning, decision making and management process, with appropriate Structures, Management and Reporting.
5. The risk management framework should:
 - (a) add value to Ministry/Department's activity and contribute to the economic, effective and efficient delivery of their objectives, at both strategic and operational level;
 - (b) reflect organisational culture and values;
 - (c) take account of the environment, both internal and external, in which the Ministry/Department operates;
 - (d) incorporate a statement committing the Ministry/Department to implement and maintain an effective, efficient and transparent system of risk management;
 - (e) define risk and risk management as they apply within the context of the Ministry/Department;
 - (f) outline the risk management approach and objectives;
 - (g) identify the key role players and their responsibilities; and
 - (h) the risk management policy should be guided by a strategy approved by the Accounting Officer.
6. The Accounting Officer of a Ministry/Department has the ultimate responsibility for risk management. To that effect, the Accounting Officers should ensure that there are adequate systems in place for identification and management of risk. The Accounting Officer may designate relevant officials with responsibility for developing the Ministry/Department's risk management framework.
7. The Accounting Officer should ensure that the Ministry/Department:
 - (a) adopts management practices in line with accountability and performance management;
 - (b) has appropriate organisational structure supported by risk management and internal controls;

- (c) objectives are finalised after thorough analysis of Inherent Risk to the Ministry/Department;
- (d) its services are appropriate, economical, efficient and equitable; and
- (e) maintain an effective process to identify the risks

Enterprise-wide risk Management (ERM)

8. ERM is a broad-based application of risk management in all major functions and activities of the Ministry/Department, rather than only in selected areas, to isolate the material risks. Thus, ERM is a concept whereby risks are managed through a portfolio/integrated approach rather than as separate.
9. Ministries/Departments should:
 - (a) identify and communicate among all public institutions the risks posed to them by the institution's own actions or inaction; and
 - (b) consider the material risks through the value chain responsible for producing and delivering particular services or goods, to appreciate the threats posed by the non-performance of the parties in the value chain.
10. Ministries/Departments must comply with various legislations that prescribe the specific treatment of risk within their ambit, for example, Occupational Safety and Health Act, National Disaster Risk Reduction and Management Act, Prevention of Corruption Act and others.

Integration of Risk Management Activities

11. Once Ministries/Departments incorporate risk assessment, implicitly or explicitly, as part of its strategic and operational decision-making process, the development and implementation of the risk management policy commits the Ministry/Department to identifying, assessing and mitigating risk and to ensuring the ongoing review and improvement of risk management approaches in a changing operational environment. Typically, the risk management strategy sets out the context for risk management within the Ministry/Department setting, the risk

management objectives, the risk management framework and process, roles and responsibilities and assurance arrangements.

12. In summary the risk management strategy helps an organisation achieve its strategic and operational objectives by managing and mitigating the risks which have the potential to affect the achievement of those objectives.
13. The risk management process should:
 - (a) address any uncertainty around the delivery of objectives;
 - (b) be based on the best available information;
 - (c) facilitate continual improvement;
 - (d) be part of decision making;
 - (e) be integral to strategic planning;
 - (f) be structured, systematic and tailored to Ministry/Department's needs; and
 - (g) be dynamic, transparent and responsive to change.
14. The objectives of a risk management policy should include:
 - (a) how to address certain risks;
 - (b) protecting the reputation of the Ministry/Department;
 - (c) improving the overall risk management framework;
 - (d) providing a level of assurance that the key legal, regulatory and governance obligations of the Department are being met; and
 - (e) ensuring that the Department is meeting the requirements of any control/governance procedures which it has in place.

Structural Configuration of the Risk Management Framework

Risk Identification

15. Risk identification attempts to identify a Ministry/Department's exposure to uncertainty. This requires a detailed knowledge of the Ministry/Department's operations and a sound understanding of its strategic and operational objectives, including a comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of these objectives.
16. The Ministry/Department should therefore adopt a rigorous and ongoing process of risk identification that also includes mechanisms to identify new and emerging risks, regardless of whether or not such risks are within its direct control.
17. To ensure comprehensiveness of risk identification, the Ministry/Department should identify risk factors through considering both internal and external factors, through appropriate processes of:
 - (a) **Strategic risk identification** to identify risks concerned with the Ministry/Department's strategic decisions:
 - (i) strategic risk identification should precede the finalisation of strategic choices to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
 - (ii) risks inherent to the selected strategic options should be documented, assessed and managed through the normal functioning of the system of risk management; and
 - (iii) strategic risks should be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.
 - (b) **Operational risk identification** to identify risks concerned with the Ministry/Department's operations:

- (i) Operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;
 - (ii) Operational risk identification should be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as management and committee meetings, environmental scanning, process reviews and the like; and
 - (iii) Subject to significant environmental and institutional changes, operational risk identification should be repeated when changes occur, or at least once year, to identify new and emerging risk.
- (c) **Project risk identification** to identify risks inherent to particular projects:
- (i) Project risks should be identified for all major projects, covering the whole lifecycle; and
 - (ii) For long term projects, the projects risk register should be reviewed at least once a year to identify new and emerging risks.

18. To facilitate Ministries/Departments to identify their internal and external risks, a list of risk categories is provided at *annex 1*.

Risk Assessment

19. Risk assessment is an integral part of risk management which provides a structured process for Ministry/Departments to identify how its objectives may be affected. It provides management with an improved understanding of risks that could affect achievement of objectives, and of the adequacy and effectiveness of controls already in place.
20. Risk assessment should be performed through a three-stage process:

- (a) **Firstly**, the inherent risk should be assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk;
 - (b) **Secondly**, risk should be expressed in the same unit of measure used for the KPIs concerned and a residual risk assessment should follow the process to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk; and
 - (c) **Thirdly**, the residual risk should be benchmarked against the Ministry/Department's risk appetite to determine the need for further management intervention, if any.
21. Risk assessment should be strengthened where possible by supplementing Management's perceptions of risk, inter alia, with:
- (a) review of external and internal audit reports;
 - (b) review of the reports of the Director of Audit and Public Accounts Committee;
 - (c) financial analysis;
 - (d) interrogation of trends in KPIs;
 - (e) benchmarking against peer group or quasi peer group;
 - (f) market and sector information;
 - (g) scenario analysis; and
 - (h) forecasting and stress testing.
22. Risk assessments should be re-performed for the risks in response to significant environmental and/or organisational changes, but at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as a result thereof.

Risk Response

23. Management should develop response strategies for all material risks, whether or not the management thereof is within the direct control of the institution, prioritising the risks exceeding or nearing the risk appetite level.
24. Where the management of the risk is within the control of the Ministry/Department, the response strategies should consider:
 - (a) avoiding the risk by, for example, choosing a different strategy or terminating the activity that produces the risk;
 - (b) treating the risk by, for example, implementing or improving the internal control system;
 - (c) transferring the risk to another party more competent to manage it by, for example, contracting out services, establishing strategic partnerships and buying insurance;
 - (d) accepting the risk where cost and strategy considerations rule out alternative strategies; and
 - (e) exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.
25. Response strategies should be documented and the responsibilities and timeline attached thereto should be communicated to the relevant persons.

Designing control activities to mitigate risks

26. As stipulated in Volume I of the Financial Management Kit, it is the responsibility of the Accounting Officer to put in place a sound system of internal control and is thus responsible to exercise care, skill, and diligence in identifying, assessing and monitoring risks.

Risk Monitoring

27. Monitoring should be effected through ongoing activities or separate revaluations to ascertain whether risk management is effectively

practised at all levels and across the Ministry/Department in accordance with the risk management policy, strategy and plan.

28. Monitoring activities should focus on evaluating whether:
- (a) allocated responsibilities are being executed effectively;
 - (b) response strategies are producing the desired result of mitigating risks or exploiting opportunities; and
 - (c) a positive correlation exists between improvements in the system of risk management and institutional performance.

Communication and Reporting

29. The Ministry/Department's risk and communication process should equip the relevant officials to identify, assess and respond to risk to support enhanced decision making and accountability through:
- (a) dissemination of relevant, timely, accurate and complete information; and
 - (b) communicating responsibilities and actions.

Accountability, Roles and Responsibilities

Risk Management Functions of Ministries/Departments

30. Responsibilities of the Ministry/Department in risk management should include:
- (a) ensuring that the Ministry/Department's strategies are aligned to the government mandate;
 - (b) obtaining assurance from management that the Ministry/Department's strategic choices were based on a rigorous assessment of risk;
 - (c) obtaining assurance that key risks inherent to the Ministry/Department are properly managed; and
 - (d) ensuring that objectives, effective performance management and value for money are achieved.

Risk Management Functions of Accounting Officers

31. The Accounting Officer is accountable for its overall governance of risk.
32. Responsibilities of the Accounting Officer to include *inter-alia*:
 - (a) setting an environment for effective management of risk;
 - (b) allocation of appropriate resources for risk management, which can include, but are not limited to human resource, documented processes and professional development;
 - (c) responsible for setting up of the appropriate internal structure and processes for risk management;
 - (d) ensuring that risk management is integrated in day-to-day activities;
 - (e) holding internal structures accountable for performance in terms of their responsibilities for risk management;
 - (f) ensuring that the control environment supports the effective functioning of risk management to properly perform their functions;
 - (g) approving the risk management policy, strategy, and implementation plan;
 - (h) approving fraud prevention policy, strategy and implementation plan;
 - (i) approving the Ministry/Department's risk appetite and risk tolerance; and
 - (j) ensuring appropriate actions are initiated in respect of the recommendations of the Audit Committee and internal audit to improve risk management.
33. Accounting Officer should also ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to risk management are assigned and communicated at all levels of the Ministry/Department.

Risk Management Functions of Audit Committees

34. The responsibilities of the Audit Committee with respect to risk management should be formally defined in its charter.
35. Audit Committees are responsible to, inter-alia:
 - (a) review and recommend disclosures on matters of risk in the annual financial statements and risk management in the annual report;
 - (b) provide regular feedback to the Accounting Officer on the adequacy and effectiveness of risk management in the Ministry/Department, including recommendations for improvement;
 - (c) ensure that the internal audit plans are aligned to the risk profile of the Ministry/Department to address the following areas:
 - (i) financial reporting risks, including the risk of fraud;
 - (ii) internal financial controls; and
 - (iii) IT risks as they relate to financial reporting.
36. In discharging its governance responsibilities relating to risk management, the Audit Committee should review and recommend for the approval of the Accounting Officer on the Risk Management Framework.

Risk Management Functions of Internal Audit

37. The role of the Internal Audit in risk management is to provide an independent, objective assurance on the effectiveness of the Ministry/Department's system of risk management.
38. Internal Audit must evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary.
39. Each Internal Audit unit must develop its internal audit plan on the basis of the key risk areas of the Ministry/Department.

40. The Internal Auditors should ascertain that the risk management processes put in place in the Ministries/Departments cover the following:
- (a) Ministry/Department objectives and mission are aligned;
 - (b) significant risks are identified and assessed;
 - (c) risk responses are appropriate to limit risk to an acceptable level;
and
 - (d) relevant risk information is captured and communicated in a timely manner to enable Accounting Officers to carry out their responsibilities.
41. When assisting Management in establishing or improving risk management processes, Internal Auditors must refrain from assuming management responsibilities for risk management.

Evaluation of Risk Management Effectiveness

Evaluation of value addition

42. Ministries/Departments should incrementally and sustainably achieve a mature risk management regime and periodically evaluate the value add of risk management by measuring outcomes against pre-set key performance indicators aligned to the overall goals and objectives.

Performance Indicators

43. Everyone in the Ministry/Department has a part to play in achieving and sustaining a vibrant system of risk management and to that extent must function within a framework of responsibilities and performance indicators.
44. The Accounting Officer should evaluate his/her own performance in leading the risk management process in the Ministry/Department through, *inter-alia*, the following:

- (a) the Ministry/Department's performance against key indicators, including comparison of year-on-year performance;
 - (b) the Ministry/Department's "avoided risk" record when compared against peer group or quasi-peer group;
 - (c) percentage change in unauthorised expenditure, fruitless and wasteful expenditure and irregular expenditure based on year-on-year comparisons;
 - (d) percentage change in incidents and quantum of fraud based on year-on-year comparisons; and
 - (e) progress in securing improved audit outcomes in regularity and performance audits.
45. With regards to the responsibilities of the Audit Committee for risk Management, the Accounting Officer should evaluate the performance of the Committee through the following and other relevant indicators:
- (a) the Director of Audit report on the effectiveness of Ministries/Departments;
 - (b) Public Accounts Committee Report
 - (c) the results the Audit Committee self-assessment;
 - (d) the pace and quality of the implementation of the risk management framework;
 - (e) the Internal Audit report on the state of risk management;
 - (f) the Audit Committee's co-ordination of the work of Internal Auditing, and other assurance providers in respect of risk management; and
 - (g) the quality and timeliness of the advice provided by the Audit Committee on risk management.
46. With regards to responsibilities of Internal Auditing for risk management, the Accounting Officer should evaluate the performance of Internal Audit through the following and other relevant indicators:

- (a) timeliness and quality of assurance on risk management;
- (b) timeliness and quality of recommendations to improve risk management; and
- (c) adoption of risk-based auditing.

Anti-Money Laundering and Combatting the Financing of Terrorism

47. On 9 July 2020, the Government of Mauritius strengthened its framework against money laundering and the financing of terrorism by passing the Anti-Money Laundering and Combatting the Financing of Terrorism (Miscellaneous Provisions) Act (the “**AML-CFT Act**”). The Act aims to align Mauritius with the recommendations of the Financial Action Task Force and the EU Commission.
48. Financial institutions must then take appropriate steps to mitigate any risks that have been identified. This will involve determining the necessary controls or procedures that need to be in place in relation to a particular part of the business in order to reduce the risk identified. The documented risk assessments that are required to be undertaken by section 17 of the FIAMLA will assist the business to develop a risk based approach.
49. Systems and controls may not always prevent and detect all Money Laundering and Terrorism Financing (ML/TF). A risk-based approach will, however, serve to balance the cost burden placed on financial institutions and their customers, with a realistic assessment of the threat of a business being used in connection with ML/TF. It focuses effort where it is needed and has most impact.
50. As money laundering risks increase, stronger controls are necessary. However, all categories of risk whether low, medium or high must be identified and mitigated by the application of controls, such verification of customer identity, Customer Due Diligence/ Enhanced Due Diligence policies, suspicious activity monitoring. A Risk Based Approach should be flexible, effective and proportionate.

51. There are three steps to establishing a Risk Based Approach: Risk Assessment, risk mitigation and risk monitoring. The following depicts the three different steps in implementing a risk based approach:

(a) **Risk Assessment** – Identify and rate the main ML/TF risks:

- (i) Customers;
- (ii) Products and services;
- (iii) Business practices/delivery channels; and
- (iv) Geographical risk.

(b) **Risk Mitigation** - Manage the business risks:

- (i) Minimise and manage the risk;
- (ii) Apply strategies, policies and procedures; and
- (iii) Put in place system and controls.

(c) **Risk Monitoring** - Conduct on-going monitoring:

- (i) Develop and carry out monitoring process;
- (ii) Keep necessary records;
- (iii) Report suspicious transactions; and
- (iv) Report to senior management.

Ministry/Department
Department Risk Management Policy

The Accounting Officer undertakes to put in place a process of risk management that is aligned to the principles of good governance.

Risk management is recognised as an integral part of responsible management and the Ministry/Department therefore adopts a comprehensive approach to the management of risk. The features of this process are outlined in the Ministry/Department's Risk Management Framework. It is expected that all departments / sections, operations and processes will be subject to the Risk Management Framework. It is the intention that these departments / sections will work together in a consistent and integrated manner, with the overall objective of reducing risk, as far as reasonably practicable.

Effective risk management is imperative to the Institution to fulfil its mandate, the service delivery expectations of the public and the performance expectations within the Institution.

The realisation of our strategic plan depends on us being able to take calculated risks in a way that does not jeopardise the direct interests of stakeholders. Sound management of risk will enable us to anticipate and respond to changes in our service delivery environment, as well as make informed decisions under conditions of uncertainty.

We subscribe to the fundamental principles that all resources will be applied efficiently, effectively and economically to ensure:

- The highest standards of service delivery;
- A management system containing the appropriate elements aimed at minimising risks and costs in the interest of all stakeholders;
- Education and training of all our staff to ensure continuous improvement in knowledge, skills and capabilities which facilitate consistent conformance to the stakeholder's expectations; and
- Maintaining an environment, which promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.

An entity-wide approach to risk management will be adopted by the Ministry/Department, which means that every key risk in each part of the Ministry/Department will be included in a structured and systematic process of risk management. It is expected that the risk management processes will become embedded into the Ministry/Department's systems and processes, ensuring that our responses to risk remain current and dynamic. All risk management efforts will be focused on supporting the Ministry/Department's objectives. Equally, they must ensure compliance with relevant legislation, and fulfil the expectations of employees, communities and other stakeholders in terms of corporate governance.

The risk policy statement shall be reviewed annually to reflect the current stance on risk management.

Every employee has a part to play in this important endeavour and we look forward to working with you in achieving these aims.

Signed: _____

Date: _____

Accounting Officer: _____

Risk Categories

Risk type	Risk category	Description
Internal	Human resources	Risks that relate to human resources of an institution. These risks can have an effect on an Ministry/Department's human capital with regard to: <ul style="list-style-type: none"> • Integrity and honesty; • Recruitment; • Skills and competence; • Employee wellness; • Employee relations; • Retention; and • Occupational health and safety.
	Knowledge and Information management	Risks relating to an institution's management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: <ul style="list-style-type: none"> • Availability of information; • Stability of the information; • Integrity of information data; • Relevance of the information; • Retention; and • Safeguarding.
	Litigation	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: <ul style="list-style-type: none"> • Claims by employees, the public, service providers and other third party • Failure by an institution to exercise certain right that are to its advantage
	Loss \ theft of assets	Risks that an institution might suffer losses due to either theft or loss of an asset of the Ministry/Department.
	Material resources (procurement risk)	Risks relating to an institution's material resources. Possible aspects to consider include: <ul style="list-style-type: none"> • Availability of material; • Costs and means of acquiring \ procuring resources; and • The wastage of material resources <p><i>*Refer to table below for potential risks associated with procurement exercise.</i></p>
	Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the citizens.
	Information Technology	The risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible

Risk type	Risk category	Description
Risk type		<p>considerations could include the following when identifying applicable risks:</p> <ul style="list-style-type: none"> • Security concerns; • Technology availability (uptime); • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology.
	Third party performance	<p>Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non-performance could include:</p> <ul style="list-style-type: none"> • Outright failure to perform; • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
	Health & Safety	<p>Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the institution; epidemic/pandemic.</p>
	Disaster recovery / business continuity	<p>Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include:</p> <ul style="list-style-type: none"> • Disaster management procedures; and • Contingency planning.
	Compliance / Regulatory	<p>Risks related to the compliance requirements that an institution has to meet. Aspects to consider in this regard are:</p> <ul style="list-style-type: none"> • Failure to monitor or enforce compliance • Monitoring and enforcement mechanisms; • Consequences of non-compliance; and • Fines and penalties paid.
	Fraud and corruption	<p>These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.</p>
	Financial	<p>Risks encompassing the entire scope of general financial management. Potential factors to consider include:</p> <ul style="list-style-type: none"> • Cash flow adequacy and management thereof; • Financial losses; • Wasteful expenditure; • Budget allocations;

Risk type	Risk category	Description
		<ul style="list-style-type: none"> • Financial statement integrity; • Revenue collection; • Increasing operational expenditure; and • Operation of cash offices (<i>*risk associated to this area is listed in table below</i>)
	Cultural	<p>Risks relating to an institution's overall culture and control environment. The various factors related to organisational culture include:</p> <ul style="list-style-type: none"> • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management style.
	Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
External	Economic Environment	<p>Risks related to the institution's economic environment. Factors to consider include:</p> <ul style="list-style-type: none"> • Inflation; • Foreign exchange fluctuations; and • Interest rates.
	Political environment	<p>Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include:</p> <ul style="list-style-type: none"> • Political unrest; • Village Council and National Assembly elections; and • Changes in office bearers.
	Social environment	<p>Risks related to the institution's social environment. Possible factors to consider include:</p> <ul style="list-style-type: none"> • Unemployment; and • Migration of workers.
	Natural environment	<p>Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as:</p> <ul style="list-style-type: none"> • Depletion of natural resources; • Environmental degradation; • Spillage; and • Pollution.
	Technological environment	Risks emanating from the effects of advancements and changes in technology.
	Legislative environment	Risks related to the institution's legislative environment e.g. changes in legislation, conflicting legislation.

Potential risk issues in relation to procurement

SN	Risk Areas	Probable Causes
1	Identifying Planning needs	<ul style="list-style-type: none"> • Understatement of the need • Overstatement of the need • Insufficient funding • Impractical target dates • Probity failure • Misinterpretation of user needs
2	Developing the Specification	<ul style="list-style-type: none"> • Narrow definition or commercial specification (eg brand name) • Definition of inappropriate product or service • Biased specification • Inadequate specification or statement of work (for services)
3	Selecting the Procurement Method	<ul style="list-style-type: none"> • Failure to identify potential sources • Selecting inappropriate method
4	Preparation of Bidding Documents	<ul style="list-style-type: none"> • Terms and conditions unacceptable to service providers • Providing inadequate information method • Bidding Process
5	Seeking, Clarifying and Closing Offers	<ul style="list-style-type: none"> • Failure to adequately address service provider enquiries • Actual or perceived favouritism in providing information • Actual or perceived breach of confidentiality • Insufficient number of responses • No response from known quality service providers
6	Evaluating Offers	<ul style="list-style-type: none"> • Failure to follow effective evaluation procedures • Breaches of security • Offers fail to meet needs • Failure to identify a clear winner Decision made on subjective grounds
7	Selecting the Preferred Service Provider	<ul style="list-style-type: none"> • Selecting an inappropriate service provider • Selecting inappropriate product

SN	Risk Areas	Probable Causes
8	Seeking, Clarifying and Closing Offers	<ul style="list-style-type: none"> • Not matching the expectations of buyer and service provider • Deadlock on details of agreement • Failure to secure mandatory conditions • Unfair or onerous requirements on the service provider in the contract conditions • Failure to reflect the terms offered and agreed in the contract • Inadvertently creating a contract without the delegate's prior approval • Inappropriate product
9	Contract Management	<ul style="list-style-type: none"> • Variations in price and foreign exchange • Unwillingness of the service provider to accept the contract • Failure of either party to fulfil the conditions of the contract • Inadequately administering the contract • Commencement of work by the service provider before contract is exchanged or letter of acceptance issued • Unauthorised increase in scope of work • Loss of intellectual property • Failure to meet liabilities of third parties (eg royalties or third party property insurance) • Loss or damage to goods in transit • Fraud • Key personnel not available
10	Disposal	<ul style="list-style-type: none"> • Collusive bidding at auction • Inadequate tender management
11	Evaluating the Procurement Process	<ul style="list-style-type: none"> • Failure to evaluate procurement and management processes • Failure to identify and address problems management

Risk Management – Operation of Cash Offices

SN	Risk Areas	Probable Responses
1	Fake Money	(i) Use Counterfeit Money Detectors in Cash Offices to ensure money collected are genuine.
2	Dishonored Cheques	(i) Establishment of proper mechanism for quick reporting of dishonored cheques and initiation of immediate action for recovery; (ii) Availability of up to date list of defaulters in cash offices; (iii) limit payment by cheque up to a certain amount and acceptance of only ‘office cheque’ for payment above the agreed amount; (iv) Use of debit/credit cards facility to limit Cash/Cheque transactions.
3	Loss/Theft	(i) Safeguard cash and cheques in a locked area prior to deposit; (ii) Prompt banking of collections and cash transit to bank under appropriate Police escort and variation of daily routes and times; (iii) Review method of lodgment of cash to Bank of Mauritius. (High risk of attack by thieves on public roads) – Department with high value daily cash collection may consider contracting out of this service to professional companies.
4	Fraud/ Embezzlements	(i) Segregation of duties - officers collecting and depositing cash/cheques should not approve remittance vouchers; (ii) Accounting of receipts and reconciliation of bank statement, holding of main stock of receipts and licenses are not to be under the responsibility of the revenue collector; (iii) Digitalization of revenue collection system. In-built system of control, Revenue collectors with authorized credentials, accountability, tracking of transactions, production of electronic receipts, etc.

Risk Management Register - Template for Ministries/Departments

Risk Type	Risk category	Risk Identification	Risk Assessment	Risk Response/ Required Actions	Risk Monitoring/ Status	Responsible Agency/Unit
Internal						
External						