



GOVERNMENT OF JAMAICA

ENTERPRISE RISK MANAGEMENT POLICY

Version 1.0

November 2019

Introduction

Public sector organisations operate in a dynamic environment of increasing volatility, complexity and ambiguity. In dealing with uncertainty, organisations need to become adaptive to change and leaders must think strategically about how to manage risks to optimize outcomes. For the Government of Jamaica (GoJ) to continually improve its approach to delivering services to its citizens, it is important that Ministries, Departments, Agencies (MDAs) and public bodies (PBs) foster flexibility, seek opportunities and focus on results. Integral to this approach is effective risk management, which is recognised as a core element of effective public administration and a critical component of sound corporate governance.

To establish the Government's framework for effective risk management, the Cabinet by way of Decision #23/18 approved an enterprise-wide approach to risk management. This Enterprise Risk Management (ERM) Policy (the "Policy") sets the structure and tone for ERM within public entities. The Policy also establishes the authority, responsibilities and accountabilities for the Head of Entity, Board, executive management and other staff.

This Policy is designed to assist government entities in meeting the requirements of the Financial Administration and Audit Act and Financial Management Regulations (2011) ("Regulations") section 144, which provides for an effective risk management process to guide the identification and treatment of risks in government departments¹. The Regulations also require that Accounting Officers shall be responsible for formulating a strategy for risk management in the public sector and for ensuring there is effective risk governance and risk management process that monitors and manages the material risks to which these entities may be exposed.

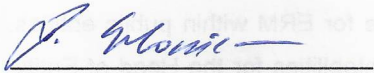
With respect to PBs, the Policy supports the Corporate Governance Framework for Public Bodies (2012). Principle 14 indicates inter alia that:

- i. Each board should put in place a formal ERM framework developed by the Ministry of Finance, to manage risk across all functional areas and business units of the Public Body;
- ii. The framework should be designed to identify, assess, prioritize, monitor and manage risks to the Public Body.

The need for risk management appears to be reasonably understood by Boards of Directors and senior management and has been implemented in a number of public bodies. However, there is the need for a more structured and formalised government-wide risk management strategy or risk management approach. The Policy, as developed, can be tailored and applied to all Government entities. The Policy addresses additional requirements and provides details of key concepts and structures for consideration.

¹ The current Regulations will be revised to include details of a more comprehensive ERM process.

The ERM Policy supports the GoJ National Development Plan Vision 2030 and is envisioned to contribute to the achievement of “Effective Governance” which is one of the expected National Outcomes. It is aligned with the Fiscal Responsibility Framework, which aims to strengthen control over expenditures by government entities, as well as to increase budget transparency. This Policy also supports the Public Financial Management Reform Action Plan, which aims to clarify, simplify, improve and harmonise the core financial management processes and information systems of the public sector.



Darlene Morrison

Financial Secretary

Table of Contents

Introduction.....	3
Glossary.....	7
1. Purpose and Objectives	12
1.1. Purpose.....	12
1.2. Objectives.....	13
2. Enterprise-wide Risk Governance Framework	13
2.1. Defining risk, risk management and enterprise risk management	14
2.2. Mission, Vision, Core Values and ERM Principles.....	15
2.2.1. Mission, Vision and Core Values	15
2.2.2. ERM Principles	15
2.3. Risk Appetite	15
2.4. Management Objectives	16
3. Managing risk within the Government of Jamaica	17
3.1. <i>Why manage risk?</i>	17
3.2. <i>Defining enterprise risk and risk management</i>	18
3.3. <i>Main principles</i>	18
3.4. <i>Risk management cycle</i>	19
3.5. <i>Risk Management Process</i>	20
3.5.1. <i>Establishing the context</i>	20
3.5.2. <i>Identifying risks</i>	21
3.5.3. <i>Analysing risks</i>	24
3.5.4. <i>Assessing risks</i>	25
3.5.5. <i>Treating risks</i>	26
3.5.6. <i>Reviewing and reporting</i>	28
4. <i>Enterprise-wide Risk Governance Structure</i>	28
4.1. <i>The Head of Entity or Board of Directors</i>	29
4.2. <i>Governance Committees</i>	30

4.2.1. Risk Management Committee.....	30
4.2.2. Audit Committee.....	31
4.3. Senior Management.....	32
4.4. General Staff.....	33
4.5. Middle Management / Head of Units (First Line of Defence)	33
4.6. Risk Management Function (Second Line of Defence).....	34
4.7. Assurance Function: Internal Audit (Third Line of Defence).....	35
4.8. External Auditors and Regulators.....	35
5. Policy Maintenance and Review.....	36
Version control.....	52
Appendix 1 - ERM Governance Structure	37
Appendix 2 - Three Lines of Defence Model.....	41
Appendix 3 - Bow Tie	43
Appendix 4 - Risk identification form.....	45
Appendix 5 - Risk typology.....	46
Appendix 6 - Impact and likelihood scoring.....	47
Appendix 7 - Risk map.....	49
Appendix 8 - Sample risk register	50
Appendix 9 - Risk appetite measures.....	51

Glossary

Term	Definition
Accept	Response to risk taken when the risk is within the organisation's risk appetite. Also known as tolerate or retain
Assurance	Evidence of certainty (or not) of existence and suitability of controls
Avoid	Potential response to a risk that is outside the organisation's risk appetite, especially where it is impossible to do anything to manage it and/or the activity that leads to it is optional. Also known as terminate or eliminate
Bow Tie	A diagrammatic way of showing the hierarchy of causes and consequences of a risk (see Annex 2 for an example)
Business Continuity Plan (BCP)	Plan to ensure continuity of business operations in the event of a serious incident that impacts the organization
Business Risk	Business risk also referred to as operational risk is related to activities carried out within an entity, arising from structure, systems, people, products or processes.
Cause	The underlying circumstances that make it possible for a risk to occur. Why a risk might occur. Ask yourself "why?" five times
Commodity Risk	This risk refers to the uncertainties of future market values and of the size of the future income, caused by the fluctuation in the prices of commodities. These commodities may be grains, metals, gas, electricity etc. Commodity risks include price risk, quantity risk, cost risk, and political risk.
Compliance Risk	The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a company may suffer as a result of its failure to comply with all applicable laws, regulations, rules, related internal policies and procedures, code of conduct and standards of good practices applicable to its activities.
Consequence	The effects of a risk occurring – so what?
Corporate Governance	A set of relationships between a company's management, its board, its shareholders and other stakeholders which provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance. It helps define the way authority and responsibility is allocated and how corporate decisions are made.
Country Risk	This risk refers to the risk of investing in a country, dependent on changes in the business environment that may adversely affect operating profits or the value of assets in a specific country. For example, financial factors such as currency controls, devaluation or regulatory changes, or stability factors such as mass riots, civil war and other potential events contribute to companies' operational risks. Country risk includes political risk, exchange rate risk, economic risk, sovereign risk and transfer risk, which is the risk of capital being locked up or frozen by government action.
Credit Risk	The risk that a borrower or counterparty, for any reason, will default on any type of debt by failing to honour its financial or contractual obligations. The risk is primarily that of the lender and includes lost principal and interest, disruption to cash flows, and increased collection costs.
Disaster Recovery	Plan for use in the event of a serious loss, such as IT failure, fire or earthquake to assist the

Term	Definition
Plan (DRP)	recovery of the organisation and support crisis management. A DRP is the initial stage of a BCP.
Financial Risk	Financial risk is an umbrella term for multiple types of risk. Financial risks create the possibility of losses arising from credit risks related to customers, suppliers and partners, financing and liquidity risks, and market risks related to fluctuations in equity prices, interest rates, exchange rates and commodity prices.
Foreign Exchange Risk	This risk is also known as currency risk or exchange risk and is a financial risk caused by an exposure to unanticipated changes in the exchange rate between two currencies.
Fraud Risk	The risk to earnings and capital due to criminal activity against the company (e.g., forgery, fraud embezzlement, theft etc).
Impact	The measurement used to assess the severity of the consequence of a risk occurring
Inherent Risk	The levels of risk before any control activities are applied, also known as gross or underlying or unmitigated. Auditors assess risks for inclusion in risk-based plans on an inherent basis
Legal Risk	Legal risk is defined as the risk of financial or reputational loss arising from: civil litigation or criminal or regulatory action; disputes for or against the organization; failure to correctly document, enforce or adhere to contractual arrangements; inadequate management of non-contractual rights; or failure to meet non-contractual obligations. These actions could significantly negatively impact an organisation's business, operations or financial condition.
Likelihood	Evaluation or judgement regarding the chances of a risk materializing.
Liquidity Risk	The risk to earnings or capital arising from situations in which a given security or asset cannot be traded quickly enough in the market to prevent a loss (or make the required profit) because parties in the market do not want to trade for that asset. Liquidity risk includes the inability to manage unplanned decreases or changes in funding sources.
Market Risk	The risk of financial losses arising from changes to the market values of asset portfolio or liabilities. Market risk includes equity risk, interest rate risk, currency risk, and commodity risk.
Mitigate	Taking actions to make a risk less severe should it occur
Near Miss	A risk that almost, but not quite, materialises. This could be because of good controls or because of good luck
Operational Risk	Operational risks are those that are likely to arise from inadequate or failed internal processes, people and systems or from external events and will have an effect on organisational operations at a non-strategic level.
Opportunities	The flip side of risk, taking advantage of circumstances to result in benefits
Owner	A risk owner takes responsibility for managing a risk although s/he may not be directly responsible for the risk actions.
Political Risk	This risk refers to the complications investors, businesses and governments may face as a result of what are commonly referred to as political decisions. That is, any political change that alters the expected outcome and value of a given economic action by changing the probability of achieving business objectives. Political risk faced by firms can be defined as

Term	Definition
	the risk of a strategic, financial, or personnel loss for a firm because of such nonmarket factors as macroeconomic and social policies (e.g., fiscal, monetary, trade, investment, industrial, income, labour, and developmental), or events related to political instability (e.g., terrorism, riots, coups, civil war, and insurrection).
Preventive Control	Type of control that is designed to eliminate the possibility of an undesirable risk materializing
Project Risk	Project risks are those that could cause doubt about the ability to deliver a project to time, budget and quality
Reduce/Treat/Control	Response to a risk that can be (further) reduced by introduction of cost-effective controls. Also known as control or mitigate
Remediation Controls	Planned actions to take after a risk has materialised to manage the after effects. This could consist of a business continuity or disaster recovery plan (see above)
Reputational Risk	Reputational risk can be defined as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect an organisation's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (e.g., through the interbank or securitisation markets). Reputational risk is multidimensional and reflects the perception of other market participants.
Residual Risk	Existing level of risk taking into account the controls already in place. Also known as current risk
Risk	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. ¹
Risk Appetite	Risk appetite is the aggregate level and types of risk that an organisation is willing to accept or take to meet its strategic objectives, deliver its business plan or take advantage of an opportunity. The level of risk appetite depends on the nature and type of activities under consideration. It is decided in advance and is intended to ensure that the organisation operates within its risk capacity.
Risk Appetite Statement (RAS)	The written articulation of the aggregate level and types of risk that an organization will accept, or avoid, in order to achieve its business objectives. It includes quantitative measures expressed relative to fiscal targets, and other relevant measures as appropriate. It should also include qualitative statements to address reputation and conduct risks as well as money laundering and unethical practices.
Risk Capacity	The maximum amount of risk an organization is able to assume given its capital base, risk management and control capabilities as well as its regulatory constraints.
Risk Context	The environment within which risks are being managed, both internal and external to the organization
Risk Culture	An organisation's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume.

¹ Institute of Internal Auditors: International Practices Framework

Term	Definition
Risk Exposure	Level of risk to which the organisation is exposed, that is the combination of the likelihood of a risk occurring and its impact
Risk Governance	Risk governance refers to the institutions, rules conventions, processes and mechanisms by which decisions about risks are taken and implemented. It can be both normative and positive, because it analyses and formulates risk management strategies to avoid and/or reduce the human and economic costs caused by disasters. Risk governance goes beyond traditional risk analysis to include the involvement and participation of various stakeholders as well as considerations of the broader legal, political, economic and social contexts in which a risk is evaluated and managed.
Risk Governance Framework	As part of the overall corporate governance framework, the framework through which the board and management establish and make decisions about the organisation's strategy and risk approach; articulate and monitor adherence to risk appetite and risk limits vis-à-vis the organisation's strategy; and identify, measure, manage and control risks.
Risk Limits	Specific quantitative measures or limits based on, for example, forward-looking assumptions that allocate the organisation's aggregate risk to business lines, legal entities as relevant, specific risk categories, concentrations and, as appropriate, other measures.
Risk Management	A process to identify, assess, manage and control potential events or situation to provide reasonable assurance regarding the achievement of the organisation's objectives. ²
Risk Map	Presentation of risk information on a grid or graph, also referred to as a risk map or heat map. It is often used to summarise the risk status of an organisation in a single diagram and is useful for reporting to senior management (see annex 4)
Risk Profile	The totality of risks faced by an organisation, considered as a whole.
Risk Register	Record of risks, the controls currently in place, the risk score, additional controls that are required and responsibility for risks and control activities (see annex 5). Separate risk registers are maintained for different aspects of organisational activities: strategic, operational, project, etc
Risk Scoring	Risk assessment process that analyses the likelihood and impact of a risk
Risk Tolerance	Risk tolerance reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve.
Risk Universe	The full range of risks which could impact, either positively or negatively, on the ability of the organisation to achieve its long term objectives.
Spotting Control	A control that will identify that a risk is about to occur and highlight this so that pre-emptive action can be taken
Sovereign Risk	The risk arising on chances of a government failing to make debt repayments or not honouring a loan agreement. These practices can be resorted to by a government in times of economic or political uncertainty or to portray an assertive position misusing its independence. A government can resort to such practices by altering any of its laws, thereby causing adverse losses to investors.
Strategic Risk	Strategic risks are long-term and/or opportunity driven and are concerned with where the organisation wants to go, how it plans to get there and how it can ensure survival. These

² Ibid

Term	Definition
	risks are very directly linked to the over-arching plans of the organization
Target Risk Score	The level of risk that it is anticipated once all planned actions have been implemented
Transfer	Response to a risk that is outside the organisation's risk appetite that can be shared with or transferred to others, by means of insurance, contract, joint venture, partnership or similar arrangements

1. Purpose and Objectives

1.1. Purpose

This Policy is a formal acknowledgement of the commitment of the GoJ to effective risk management. It aims to ensure that public entities use a consistent approach to effectively manage risk, balance exposure against opportunities with the goal of enhancing capabilities to create, preserve, and realize value for their stakeholders.

The GoJ considers ERM to be integral to its operations as it helps to improve decision making in governance, strategy, objective setting and day-to-day operations of its entity. It also helps to enhance performance by more closely linking strategy and business objectives to both risk and opportunity. As such, ERM principles shall be integrated into all aspects of the GoJ's operations - both at the strategic and operational level - to include governance, strategy, performance management, and internal control.

This Policy applies to all public officers and requires all employees to understand the nature of risks and accept responsibility for managing risks in their area of authority. The GoJ has adopted the international standard for risk management ISO: 31000 as its ERM framework.

The ISO 31000 Risk Management Framework is anchored on eight principles, which are:

- 1) The ERM strategy should be customized and proportionate to the type of organization.
- 2) Appropriate and timely involvement of stakeholders is necessary.
- 3) Structured and comprehensive approach is required.
- 4) Risk management is an integral part of all organizational activities.
- 5) Risk management anticipates, detects, acknowledges and responds to changes.
- 6) Risk management explicitly considers any limitations of available information.
- 7) Human and cultural factors influence all aspects of risk management.
- 8) Risk management is continually improved through learning and experience³

³ Source: Institute of Risk Management (2018), "A Risk Practitioners Guide to ISO 31000"

1.2. Objectives

The objectives of ERM in the GoJ are to:

- Enhance management’s ability to select a strategy that aligns anticipated value creation with the entity’s risk appetite and its capabilities for consistently managing risks;
- Embed ERM practices within the strategy-setting and operational processes of public entities so that risks are consistently managed in accordance with the GoJ’s values, in a pragmatic and cost-effective way;
- Proactively anticipate changes to the operating environment (rather than reactively manage the outcomes) that may impact achievement of the entity’s strategic objectives and implement an effective risk mitigation strategy; and
- Enhance management decision-making so that it can be determined whether decisions create, preserve, realize or erode value for the entity.

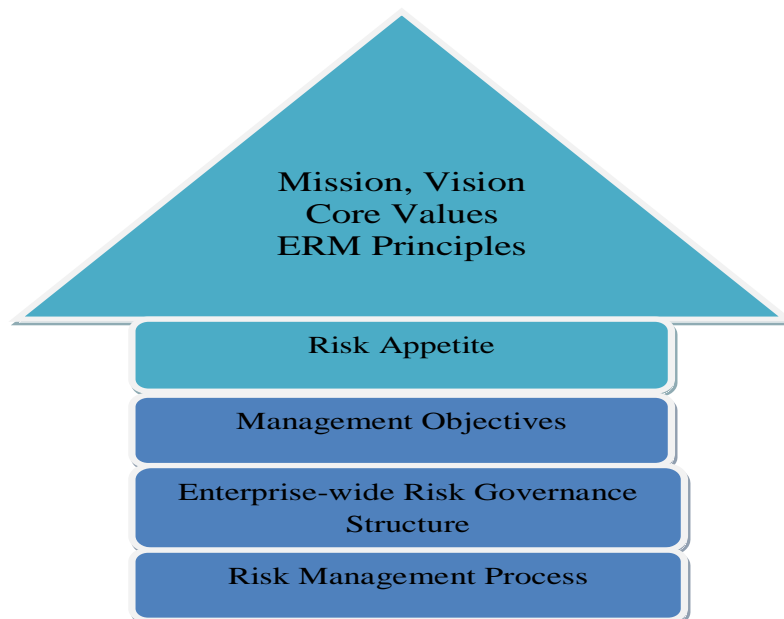
2. Enterprise-wide Risk Governance Framework

The GoJ has developed a comprehensive enterprise-wide framework for risk governance (the ‘Framework’), which, together with culture, forms the foundation for the effective operation of ERM. Culture reflects the organization’s ethics: the values, beliefs, attitudes and understanding of risk. It supports the achievement of the organization’s mission and vision and the GoJ embraces a risk-awareness culture, which emphasizes the importance of managing risk and encouraging a transparent and timely flow of risk information.

The Framework sets out the GoJ’s enterprise-wide approach to managing risks across public entities. It comprises the following key interrelated components, which are presented in **Figure 1** and discussed in the following sections:

- Defining risk, risk management and enterprise risk management – **Section 2.1**
- Mission, vision, core values and guiding ERM principles – **Section 2.2**
- Risk appetite – **Section 2.3**
- Management objectives – **Section 2.4**
- Managing Risk in the GoJ – **Section 3**
- Enterprise-wide Risk governance structure - **Section 4**

Figure 1. GoJ Enterprise-wide Risk Governance Framework



2.1. Defining risk, risk management and enterprise risk management

Term	Definition
Risk	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. ⁴
Risk management	A process to identify, asses, manage and control potential events or situation to provide reasonable assurance regarding the achievement of the organization's objectives. ⁵
Enterprise Risk Management	The culture, capabilities and practices, integrated with strategy-setting and its execution that organizations rely on to manage risk in creating, preserving, and realizing value. ⁶

⁴ Institute of Internal Auditors: International Practices Framework

⁵ Ibid

⁶ Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2016). Enterprise risk management. Aligning risk with strategy and performance (Public Exposure Draft)

2.2. Mission, Vision, Core Values and ERM Principles

2.2.1. Mission, Vision and Core Values

The mission and vision of the GoJ should provide a high level indication of its risk ‘appetite’ in terms of the acceptable type and amount of risk the government will pursue to achieve its objectives. They help to establish boundaries and focus on how decisions may affect strategy. The GoJ’s strategy is aligned with its mission, vision, and core values to realize its objectives.

The Head of Entity or Board and senior management have overall responsibility for the organization, including the approval and oversight of management’s implementation of the GoJ’s ERM strategy and governance framework. The Head of Entity or Board and senior management should set the ‘tone at the top’ and oversee management’s role in fostering and maintaining a robust risk-awareness culture.

2.2.2. ERM Principles

The Framework is established on the following overarching ERM principles, which should guide decision-making throughout the organization. Individually, each principle is equally important, and taken as a whole, they form GoJ’s risk management philosophy. They sit alongside the operational principles described in the ERM User Guide:

- GoJ will establish a strong and supportive tone that is communicated from the top of the organization in support of an ethical risk-awareness culture;
- Management will define and establish the organization’s risk appetite in the context of creating, preserving and realizing value for its stakeholders;
- Management will ensure effective ERM practices are embedded at the strategic and operational levels of the organization; and
- MDAs and public bodies will prioritize risks in order to inform decision-making and optimize allocation of resources.

2.3. Risk Appetite

An effective risk governance framework includes a strong risk culture, a well-developed risk appetite⁷ articulated through a Risk Appetite Statement (RAS), and defined roles and responsibilities for risk management and control functions. The RAS establishes, at the individual and aggregate level, the major risks the GoJ entity is willing to assume in advance of and in order to achieve its strategy and business objectives. The RAS includes limits, targets and measures for evaluating performance

⁷ Although risk appetite is referred to in the singular, in practice the GoJ will have a variety of risk appetites depending on the context within which they work and across appropriate dimensions.

against the risk appetite and the overall risk profile, which provides a composite view of the risk at a particular level of the entity or aspect of the business model. The RAS should be communicated throughout the organization and shall be monitored and evaluated by the risk management function on an ongoing basis to ensure its appropriateness. (see **Appendix 9**). Each Ministry should develop a RAS by their senior management and approved by the Head of Entity or Board as applicable in line with the overall Government of Jamaica's RAS (GoJ's RAS can be accessed at <http://www.mof.gov.jm/documents/documents-publications/document-centre/file/1967.html>).

The overall risk appetite of the GoJ is outlined in the Fiscal Responsibility Paper (Fiscal Risk Statement) and provides guidance to government entities on the collective approach to risk; and provides a common understanding among all stakeholders of how risk appetite should be established and managed. The GoJ's RAS communicates the overarching risk appetite for all government organization; therefore, the management team should link it to daily operational decision-making and establish the means to raise risk issues and strategic concerns. Risk and related resources are to be carefully managed in order to achieve the metrics established in the RAS.

2.4. Management Objectives

This Policy is designed to ensure the risk management and internal control environment are appropriately structured and adequate to mitigate risks the organization undertakes to achieve its objectives. The Policy is designed with four categories of objectives, which allows management to focus on the key areas of the organization. These objectives are:

Strategic Objectives: These are high level objectives which are designed to achieve the GoJ's mission, vision and core values. For risk management and internal control purposes, these objectives address the strategic objectives of the GoJ as well as its overall risk appetite. The strategic objectives outline the direction of the GoJ and set the tone for the risk management and control policies.

Operational Objectives: These objectives relate to the effectiveness and efficiency of the GoJ's operations, including operational and financial performance goals, and safeguarding assets against losses. The risk management and internal control processes seek to ensure that personnel throughout the GoJ are working to achieve its objectives without unintended or excessive costs or placing other interests (e.g., employees, vendors or other stakeholders) before those of the GoJ.

Reporting Objectives: Reporting objectives address the preparation of timely, reliable reports required for decision-making. Reliable reporting also addresses the need for credible financial statements and other financial and non-financial related disclosures, including regulatory reporting, other external and management reports. The information received by management, the Head of MDAs and Board of PBs should be of high quality and integrity so that users can rely on the information in making decisions. Effective risk management will increase the likelihood of reliable reporting by identifying and managing areas of uncertainty.

Compliance Objectives: These objectives ensure all the activities of the GoJ are conducted in compliance with applicable laws and regulations, and the GoJ's policies and procedures. The compliance objectives contribute to protecting the GoJ's reputation, which is also one of the principle aims and benefits of good risk management.

3. Managing risk within the Government of Jamaica

Private or public, no organization operates in a risk-free environment. The nature, mandate and services of the Government of Jamaica (GoJ) mean that it carries out its work in an environment that can be complex and unstable, which exposes it to both risks and opportunities. The approach to risk management aims to facilitate your approach to risk and to increase the GoJ's ability to identify and manage the risks that may affect the achievement of its objectives. It also aims to help make the most of opportunities that may present themselves.

This guidance is intended for anyone who is tasked with identifying and managing risks. It will give you a practical, structured and pragmatic approach to risk identification and management that will work alongside your current management activities and not be overly burdensome and bureaucratic.

3.1. Why *manage risk*?

The risk policy states that: risk management is recognized as a core element of effective public administration and a critical component of sound corporate governance. For the GoJ to continually improve its approach to delivering services to its citizens, it is important that its Ministries, Departments and Agencies (MDAs) foster flexibility, seek opportunities and focus on results. Integral to this approach is effective risk management which provides the flexibility to MDAs to design solutions to achieve their mandates and objectives

In managing risk, the aim is not to remove risk or to reduce it at all costs but to identify and implement sensible, balanced, proactive measures that will increase the likelihood of delivering plans and realizing opportunities. Ultimately, risk management is good management. By seeking to identify, prioritize and manage the risks that could impede the achievement of objectives and aiming to identify those actions that make it easier to make the most of opportunities and achieve objectives, the GoJ will be able to deliver what it has committed to deliver in a more efficient and effective manner.

3.2. Defining enterprise risk and risk management

Good risk management supports you in being proactive in recognizing and managing uncertain events that have an effect on objectives. It supports the reduction of negative consequences, helps you to seize opportunities and, ultimately, improves your chances of reaching objectives within budget and timeline.

Term	Definition
Risk	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. ⁸
Risk management	A process to identifying, assessing, managing and controlling potential events or situation to provide reasonable assurance regarding the achievement of the organization's objectives. ⁹
Enterprise Risk Management	Enterprise risk management is defined as the culture, capabilities, and practices, integrated with strategy-setting and its execution, that organization rely on to manage risk in creating, preserving, and realizing value. ¹⁰

3.3. Main principles

Risk management is about being aware of the risks that you face and taking deliberate and agreed decisions on how to deal with them. The approach follows these principles:

- **Anticipate and manage risk:** when developing strategies, action plans, work plans, designing or reviewing programmes, projects or activities, all staff should consider risks to the achievement of the expected results
- **Avoid unnecessary risk:** there is no benefit in taking a risk that does not help achieve objectives. You should be able to link all of your risks to activities that will support delivery of the GoJ's objectives. If you are undertaking activities that do not contribute to this, you are potentially exposing the GoJ to unnecessary risk
- **Accept risk where the benefits outweigh the cost, both financial and otherwise, of eliminating or reducing it:** total risk elimination may not be possible or can be impractical and is not the aim of risk management. Instead, take a balanced view of your risks, seek to understand them and manage them in an appropriate fashion, taking value for money into account

⁸ Institute of Internal Auditors: International Practices Framework

⁹ Ibid

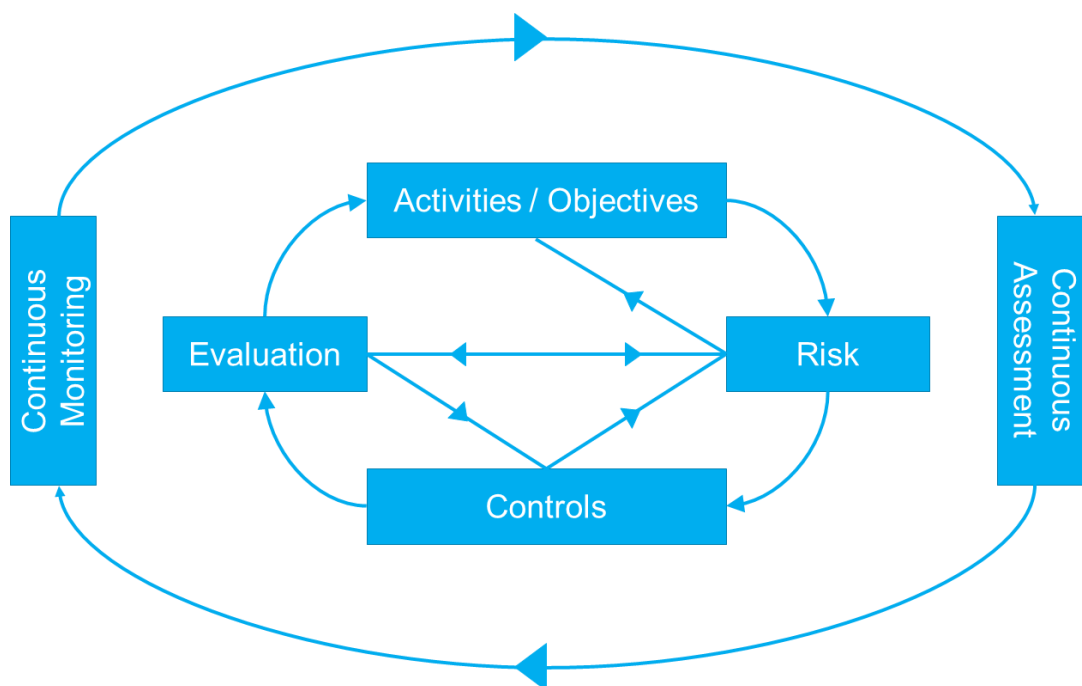
¹⁰ Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2016). Enterprise risk management. Aligning risk with strategy and performance (Public Exposure Draft)

- **Make risk management decisions at the right level:** take decisions on risk at the appropriate level so that effective action can be taken. Do not accept risks where you do not have the necessary authority and escalate risks to higher levels of management as necessary
- **Do not take risk management as an exact science:** it is based on professional judgement and will support good management practices.

3.4. Risk management cycle

Risk management is a cyclical process that involves many reiterations. The diagram below shows the risk cycle, indicating both the main flow of the process but also the mini-cycles within the overarching cycle. The speed with which you progress around this cycle depends on the types of risks that you are evaluating. If they are high-level, corporate risks, the cycle may be spread over some time, perhaps up to a year. If, however, you are dealing with faster-moving more operational risks, the cycle will also be faster moving, perhaps as fast as daily for some risks (project risks for example). You will need to determine the appropriate timing for your particular risk cycle.

Figure 1: Risk Management Cycle

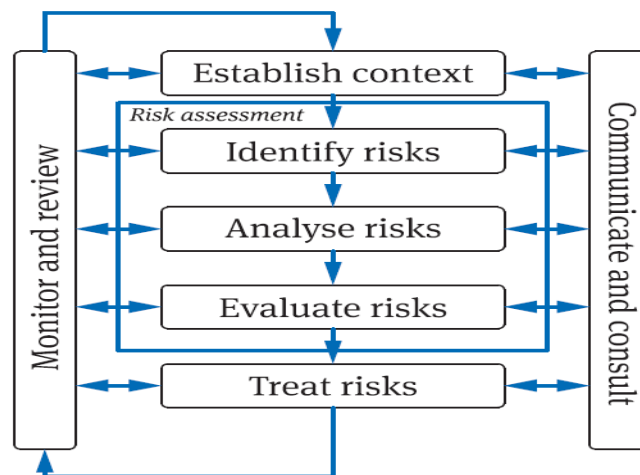


3.5. Risk Management Process

The risk management process is organized into six main stages, shown in Figure 2. A full description of the objectives of each stage and the methods of implementation are set out in the ERM Guidelines that accompany this document:

1. Establishing the context
2. Identifying risks
3. Analyzing risks
4. Assessing / Evaluating risks (their likelihood and potential impact)
5. Treating risks (by taking positive action to manage their likelihood and/or impact)
6. Reviewing and reporting / communicating on risks

Figure 2. Risk Management Process¹¹



3.5.1. Establishing the context

Before you start a risk identification exercise, you must decide exactly what is being risk appraised and thus, who should be involved and what they should be considering. It is also important to consider the context, both external and internal.

3.5.1.1. What is being risk appraised?

There are many different types and levels of risk and it is more effective to consider similar and connected risks together to focus the process. Start by identifying exactly what aspect of your MDA is being risk appraised. This could be:

¹¹ Adapted from The ISO 31000: 2009 Risk Management Process

- The strategic risks that could affect the overall delivery of your MDA;
- A particular project or programme;
- A specific aspect of your activities, for example IT or recruitment;
- The operations of a single unit; or
- A specific theme, for example fraud.

Once these parameters have been set, you can then decide who it would be best to involve.

You will also need to decide when to carry out the exercise: some risk appraisals are time-sensitive (for example, a strategic risk assessment is linked to the annual planning cycle) or may need to be carried out at specific stages in a project. Others will have no obvious timing requirements and so will need to be fitted into the normal work programme.

3.5.1.2. External context

The external context is anything that is happening beyond the Government of Jamaica or beyond your particular unit or division that may have an impact on your activities and risks. It could be something tangible, for example demographic change or something intangible, for example changes in the expectations of the Government by the electorate. It is impossible to produce a definitive list of matters to consider, so you will have to think widely and consider the implications of anything that you identify. You may want to revisit this list when you are identifying risks.

3.5.1.3. Internal context

The internal context is anything that is happening within the Government of Jamaica, especially within your division, that may affect your activities and risks. Consider both before the risk identification exercise but also as part of your risk identification. The key aspects are:

- What are your objectives (for the section, project and activity that you are risk appraising)?
- What is your capacity to do something about the risks that you identify, to absorb shocks and manage the unexpected? For example, is there a financial contingency that you could draw upon? Or do you have staff that could be redirected in case of a problem?
- What is already built into your current business processes and what else can you build in?
- Do your decision-making processes allow for a speedy reaction to events or do you need to build in early-warning systems to alert you to potential risks in time to take action?

3.5.2. Identifying risks

The starting point of any risk identification exercise is the objectives of the area being risk appraised together with any relevant matters highlighted when considering the context (above). It is then a matter of working with others, using both your knowledge of the business and your imagination, to

identify what will make it more likely that you will achieve your objectives and what might get in the way of doing so. It is crucial that you obtain multiple perspectives on your risks and so involve the relevant colleagues identified in 2.1.1 above.

There are many techniques used to identify risks, some of which are given below. Use them individually or, preferably, in combination:

- Consult colleagues through brainstorming, workshops, etc. The best risk assessments always obtain a multitude of perspectives. Some questions for a workshop include:
 - What keeps you awake at night?
 - What must you deliver?
 - What could get in the way of achieving your objectives?
 - What are you choosing to ignore?
 - What are your assumptions and are they realistic?
 - What is the 'elephant in the room'?¹²
- Identify key milestones and consider events that could throw you off course or that are critical to help you achieve milestones and objectives;
- Ask "what if?" questions:
 - What if a supplier goes bankrupt?
 - What if there is a sudden change in the political situation in a country that is supporting us in delivering this project?
 - What if the necessary expertise is not available within the required timeframe?
- Consider the history of risks and incidents in your area of work and the likelihood of similar events happening in the future;
- Consider what 'near misses' have you had recently;
- Consult relevant evaluations and audit reports; and
- Keep the focus high-level so that you identify the material risks rather than those that are known about and dealt with in everyday processes.

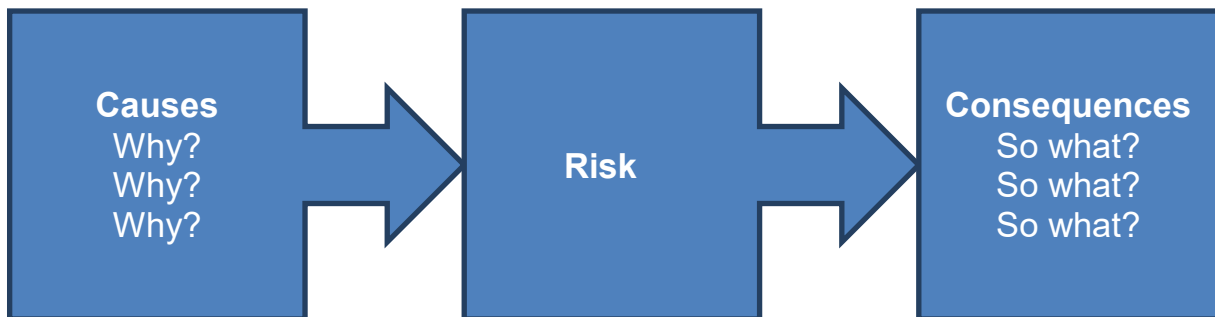
It is important at this point to spend time focusing on the exceptions rather than the norms, brainstorming the less obvious risks. Avoid re-using previous risk assessments as these may limit your thinking so that you do not look beyond the expected. Challenge and question assumptions: are they too optimistic or pessimistic (there is often an optimism bias in projects and plans)?

¹² These are the risks that everyone is aware of but never talks about, perhaps because they are too uncomfortable, or politically sensitive or just something that it is thought nothing can be done about. These risks can be the most troublesome to manage and have significant consequences if they occur.

3.5.2.1. Describing risks

Once identified, a risk must be clearly described. This will enable you both to assess its magnitude and, more importantly, to develop actions that are likely to manage it effectively. A good risk description will:

1. Provide a clear link to the objective(s) that it might affect;
2. Explain both why it is a risk (the causes) and why it matters (the consequences);
3. Look beyond the obvious and explore underlying causes and subsequent consequences;
4. Be more than just a statement of the opposite of the objective



3.5.2.2. Causes

Risks almost always have more than one cause and the causes may be immediate (the event that finally causes the risk to materialize) or underlying. For example, if a bridge fails, the immediate cause could have been an over-weight vehicle crossing or particularly bad weather conditions but there will have been underlying weaknesses that meant that it couldn't cope with these (relatively insignificant) events. These underlying weaknesses could have been poor workmanship, substandard materials or an inappropriate design. Indeed, it could be a combination of all three of these and other factors too. When you are describing causes, keep asking "why might this happen?" until you either run out of ideas or reach an act that is beyond your control.

It is helpful to understand the hierarchy of the causes that you have identified i.e. because of one thing, then another happened and because of those two things, something else occurred. It can be difficult to combine all of the causes into a single coherent sentence, so you might find it easier to draw the causes as a 'Bow Tie' (an example, with guidance, is provided in Appendix 3), or to list them out as bullet points in a logical order (a form for capturing this information is provided in Appendix 4).

3.5.2.3. Consequences

Just as risks will usually have more than one cause, they will also almost always have more than one consequence, and these will also take the form of immediate or subsequent consequences. In the example of the bridge collapsing, the immediate consequences will be loss of a crossing point and

death or injury to whoever was on the bridge at the time. Subsequent consequences may include the chaos for traffic in the area, loss of business for local companies because clients can't reach them, lawsuits from those affected and professional damage for those involved in designing and building the bridge. When you are describing consequences, keep asking "so what?" until you either run out of ideas or reach a consequence that is beyond your responsibility. It is helpful to understand the hierarchy of the consequences.

3.5.2.4. Grouping risks

Risks are grouped to identify common themes, risks that are more effectively dealt with together and risks that cross organizational boundaries. They are also grouped according to their effect on objectives so that it is clear where the greatest threats lie. The risk typology used by the GoJ is set below (see details at **Appendix 5**):

- **Political:** risks relating to political matters
- **Economic:** risks relating to financial matters
- **Sociological:** risks relating to social change and social matters, demographics, etc.
- **Technological:** risks relating to IT especially, but also anything with a significant technical component
- **Legal:** risks which might give rise to a legal challenge or where legal matters are being examined
- **Ethical:** risks relating to people and their behaviours
- **Environmental:** risks that might give rise to environmental harm
- **Assets:** risks relating to our infrastructure and equipment
- **People:** risks relating to staff, their behaviours, culture, etc.
- **Reputation:** risks that could give rise to reputation damage
- **Information:** risks relating to information management and the use of information
- **Continuity of Operation:** risks that could threaten the activities that underpin our day-to-day business

Risks may not fit neatly into one category, but you should use a "best fit" approach to enable an effective comparison of risks and identification of common themes.

3.5.3. Analysing risks

The next stage after describing risks is to identify what is already being done to manage them. It is likely, unless this is a completely new activity, that there will already be controls in place to address both the causes and the consequences. Identifying these existing controls and considering their effectiveness is an important step in risk prioritization.

3.5.4. Assessing risks

There are three levels of appraising risk: inherent, current (or residual) and target. Except in the rare cases where statistical data are available, risk scoring is not an exact science but is based on combined knowledge and informed judgement against agreed parameters. The clearer your risk description, including the causes, consequences and current controls, the better your judgement will be. There are three levels at which a risk can be assessed:

- **Inherent risk** is the level of risk faced when no controls are in place. This is the approach to risk scoring used by internal audit as it enables them to focus on those areas where failing controls could lead to the greatest risk. It is not used for risk management purposes in the GoJ but is included here for clarity;
- **Current risk** (also known as residual) is the level of risk that is currently faced with the controls that are currently in place, considering how well (or not) those controls may be working. Recording this score enables you to prioritize risk activities to manage your more significant risks;
- **Target risk** is where you anticipate the risk score will be when the actions that you have planned have been fully implemented. Recording this score will enable you to assess the value of the actions that you are planning to take to manage risk and identify those that may be superfluous or which do not yield sufficient value

Risks are scored on two parameters: likelihood and impact, with risk prioritization weighted towards impact.

Likelihood is scored considering the frequency of an event, on a scale of 1 to 4. Further details of this scale are provided at **Appendix 6**.

Impact is assessed through a judgement of the potential outcome should the risk materialize, considering the impact on delivering objectives, reputation, financial loss, human resources and ability to operate. Impact is scored on a scale of 1 to 4. Further details of this scale are provided at **Appendix 6**.

A risk may have a major impact when it occurs, but the likelihood of it happening may be very remote. Conversely, a risk with a minor impact may become a major risk if it occurs repeatedly. Bringing these two parameters together calculates the total risk exposure and enables risks to be compared with each other. Each risk is plotted on a risk map for each of these two scales, and assigned a Low, Medium or High rating, which determines the risk treatment to be adopted (see section 3.5.5.2). The risk map is provided at **Appendix 7**.

3.5.5. Treating risks

Depending on the level of exposure and risk appetite, you must take a decision on whether to:

- Accept the risk; or
- Treat the risk by:
 - Avoiding it:
 - Transferring it: or
 - Reducing it.

3.5.5.1. Accepting the risk

A risk is deemed to be acceptable if it is not going to be treated. Accepting a risk does not imply that it is insignificant. You may decide that it is appropriate to accept it for a number of reasons:

- The level of the risk is so low (very unlikely to happen and/or with a very low impact) that based on, for example, a cost benefit analysis, specific treatment is not considered appropriate;
- The risk is such that no treatment option is available. For example, the causes may be beyond the control of the Government of Jamaica or there simply may be nothing that can be done other than manage the outcome of the risk should it happen; or
- The opportunities presented outweigh the threats to such a degree that accepting the risk is justified, perhaps after some action has already been taken to mitigate it to an acceptable extent.

3.5.5.2. Treating the risk

There are three basic methods of treating risks:

3.5.5.2.1. Avoiding the risk

This is achieved either by deciding not to proceed with the activity that creates the risk, choosing an alternative, more acceptable activity that meets your objectives and goals, or choosing an alternative and less risky methodology or process within the activity. This is likely to address the causes of the risk.

3.5.5.2.2. Transferring the risk

Risk transfer moves some or all of the risk to an outside party. The most common method of risk transfer is through insurance, but contracts and partnership arrangements may also be a form of risk

transfer. Remember that there may be some element of risk remaining: transferring reputation risk, for example, is almost impossible. This may address the causes and/or the consequences of the risk.

3.5.5.2.3. Reducing the risk

Risk control focuses on reducing the likelihood of the risk occurring and/or its impact should it occur. There are four main approaches;

1. Ideally you will seek to **prevent** the risk from occurring by barrier-type controls that address the underlying causes of the risk. Passwords on computer systems are an example of a preventative control;
2. If you cannot prevent, try to **spot** that the risk is about to occur and take pre-emptive action by addressing the immediate causes of the risk. Anything with an alarm or warning gauge is a spotting control;
3. If you cannot address the likelihood, address the impact with **mitigating** controls that make the impact less severe i.e. addressing at least some of the consequences of the risk; or
4. If you can do nothing to prevent the risk from happening or make it less severe as it happens, ensure that you have good **remediation** controls in place. For example, disaster recovery and business continuity plans minimize the consequences of a risk once it has occurred.

Your mitigation plans should include:

- Proposed actions;
- A named individual responsible for implementing the actions; and
- A timetable, including deadlines by which each action should be implemented and dates for progress review.

There is a tendency to implement actions simply because they can be done or because it makes it look as if action is being taken. It is vital to identify the actions that will really make a difference and bring the risk down to acceptable levels, especially the causes of the risk. To assist with this, we record the 'target' risk score i.e. the expected risk exposure with all planned actions completed and working as anticipated.

3.5.5.3. Assurance on risk

Assurance on risk is how you and your managers know that current and future controls are managing, or will manage your risks. Assurance is the evidence that underpins controls and it can be positive (you know that the controls are working because they've been checked) or negative (you think that these controls are working because you haven't had any problems yet). Clearly positive assurance is preferable to negative assurance.

When describing current controls you should also describe the assurance that you have or need to demonstrate that it is working i.e. how would you know that this control is in place? If there is currently

no assurance, positive or negative, you should identify something that could be added to the control framework to deliver this. Similarly, you will need assurance on planned actions to be sure both that they are progressing as planned and also that they will deliver the control that is anticipated. The model used to identify and assess the value of assurance is the Three Lines of Defence (details of which are given at **Appendix 2**).

3.5.6. Reviewing and reporting

The basic risk management tool is a risk register, which records the risk and its owner¹³, its causes and consequences, current and planned controls and risk scores. A risk register template is included at **Appendix 8**. The GoJ maintains a number of risk registers:

- **Government-wide**, which mainly consists of those risks that have been escalated by MDAs, those risks that cross MDAs and are best dealt with jointly and those risks that affect the country as a whole;
- **Corporate i.e. at MDA level**, including those risks that could cause the MDA to cease to operate;
- **Operational**, including departmental, divisional and unit risk registers, to capture and manage the risks faced at each of these levels;
- **Project**, for every project and programme undertaken within the GoJ.

4. Enterprise-wide Risk Governance Structure

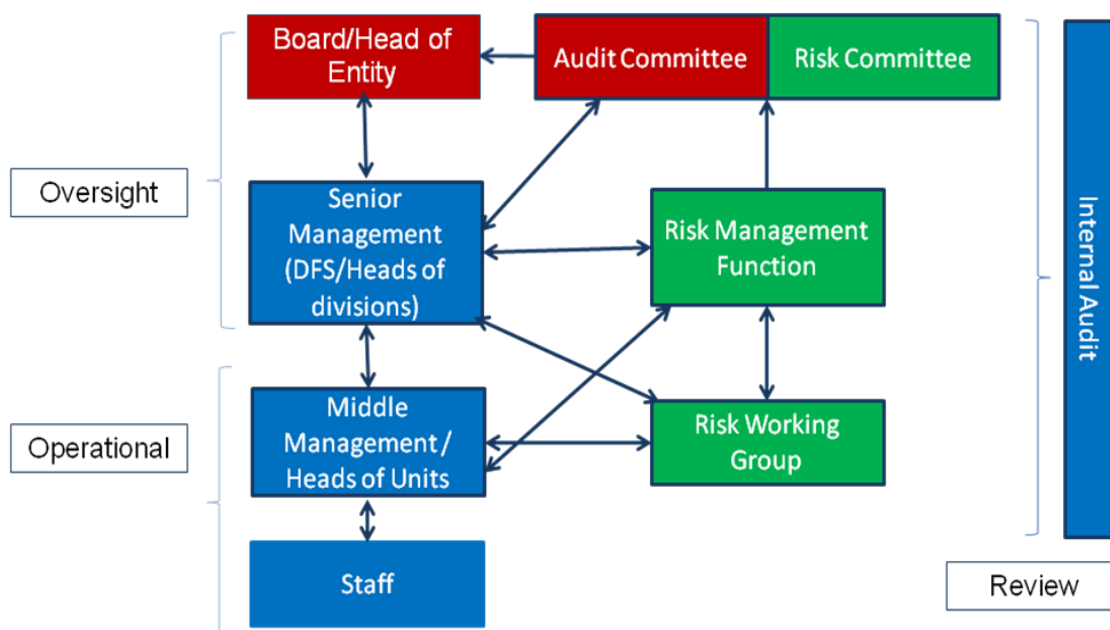
Risk governance is an integral aspect of the GoJ's corporate governance. It focuses on structures, processes and approaches to the management of significant risks to the MDA's and public bodies' strategy and business objectives and is used by the GoJ as the system for directing and controlling the management of risk. The GoJ's Risk Governance Structure includes distinct roles with oversight, operational and review responsibilities. These roles and responsibilities are closely aligned to the Three Lines of Defence Model. The tailored GoJ governance structure is described in Section 4.1 – 4.8 (summary provided at), with specific reference to the Three Lines of Defence as relevant. Further details are provided at **Appendix 2**.

¹³ A risk owner takes responsibility for managing a risk although s/he may not be directly responsible for the risk actions.

Roles and Responsibilities

All employees are required to play an active role in managing risk, fostering a positive risk management and control environment, and a robust risk-awareness culture within the GoJ. A detailed description of the roles and responsibilities are described below.

Figure 3. GoJ's Risk Governance Structure



4.1. The Head of Entity or Board of Directors

The Head of Entity or Board have oversight responsibilities and accountability for an effective risk governance framework. This includes a strong risk culture, a well-developed risk appetite articulated through the RAS, and well defined responsibilities for risk management and control functions. The Head of Entity or Board should ensure the risk management functions are properly positioned, staffed and resourced and that they carry out their responsibilities independently, objectively, and effectively. They should ensure that there are regular reviews of key policies and controls, confirming that they are identifying and addressing significant risks. They should also make decisions on whether adequate controls are in place to manage risk exposure to acceptable limits.

Roles and Responsibilities of the Head of Entity or Board of Directors

- Lead by example in integrating the GoJ's risk management culture and values by promoting a risk-awareness mindset throughout the organization;
- Understand the MDA's/ public body's environment/industry strategy and operating model and the issues, challenges and risks that it faces. Establish, along with senior management, the

entities' risk appetite(s), taking into account its long-term interests, risk exposure and ability to manage risk effectively;

- Monitor the entities' exposure to key risks that could adversely impact its strategy, reputation or long-term viability. Engage in regular discussion with management to understand any change to the organization's context that may impact the strategy and result in new or emerging risks. Consider whether or not the resultant risk exposure is consistent with the organization's risk appetite;
- Oversee alignment of business performance, risk taking, and incentives/compensation to balance short-term and long-term strategic achievement;
- Require management to demonstrate an understanding of the risk capacity of the entity to withstand large, unexpected events;
- Approve and oversee the MDA's, public body's risk management policy and governance framework. Periodically¹⁴ conduct or commission a review to ensure it remains appropriate in light of material changes to the organization's size, complexity strategy, experiences of and developments in risk management;
- Approve and oversee key risk management processes. Understand how risk is monitored by management and challenge them to demonstrate that risks relevant to the organization are being properly identified and managed;
- Monitor to ensure management's actions with regards to the most significant risks are consistent with the strategy and policies approved by the Head of Entity or Board;
- Review periodic reports from the Risk Management Function / Risk Management Committee and discuss, request and approve suggested actions.

4.2. Governance Committees

To increase efficiency and allow deeper focus in specific areas, the Head of Entity or Board establishes specialized Committees to assist in discharging their responsibilities. The Head of Entity or Board may give oversight authority to these Committees but they may not delegate their responsibilities.

4.2.1. Risk Management Committee

The Risk Management Committee (RMC) assists the Board/Head of Entity in achieving its risk management and control responsibilities. It has a Charter which outlines its mandate, scope and responsibilities, as well as its working procedures. It oversees and challenges the operation of ERM within the entity and the risk and control information presented to it, including the appropriateness of

¹⁴ At least annually, or whenever a significant change occurs.

the organization's risk appetite and risk exposure, the control actions being taken to manage key risks and the strength of risk culture. Their specific responsibilities include to:

- Foster and promote a strong risk-awareness culture by setting the 'tone at the top.' Encourage open and transparent discussion of risks. Monitor the risk culture and advise the Head of Entity/Board on any action that should be taken to strengthen the organization;
- Review, challenge and advise the Head of Entity/Board on the organization's risk appetite statements. Discuss their continuing appropriateness and make recommendations for change as necessary;
- Oversee the organization's processes for comparing overall risk exposure to risk appetite and monitor / challenge any occasions where the two are not aligned;
- Review the activities and structure (including resources) of the risk management function. Advise the Head of Entity/Board if these are inadequate;
- Keep under review the effectiveness of the design of the ERM framework and processes, including assessment parameters. Make recommendations for any necessary change;
- Keep under review the effectiveness of the operation of the ERM framework and processes, considering whether it ensures that all key risks are identified and effectively managed;
- Ensure that risk is considered in all major decisions – including in the strategic planning process and the approval process for new programmes, activities, processes and systems;
- Discuss strategies taken to manage risk, both on an aggregated basis and by material risk type, in order to ensure management actions keep risk exposure within the stated risk appetite;
- Monitor management action of agreed solution to manage material risks; and
- Review periodic reports on:
 - material issues regarding risk management (internal audit reports);
 - material risk breaches and the adequacy of proposed action (internal audit and / or management reports); and
 - key metrics agreed with management regarding aspects such as the organization's current risk profile, the state of risk culture, compliance with risk limits and progress on mitigating action plans (Risk Management function).

4.2.2. Audit Committee

The Audit Committee oversees the financial reporting and internal control of the MDA and public bodies. The Committee has responsibility to monitor and review the activities of internal audit, ensuring that it has the necessary resources and access to information to perform its role. The Committee ensures the financial activities of the MDA and PBs are subject to independent review and external audit, and for self-financed PBs appointing the external auditor and monitoring their independence, objectivity, and cost effectiveness. The Audit Committee has responsibility to:

- Foster and promote a strong risk-awareness culture by setting the 'tone at the top.' Encourage open and transparent discussion of risks;

- Advise the Head of Entity or Board on the integrity of the financial reporting and the effectiveness of the internal control system;
- Monitor and review the activities of internal audit, ensuring the internal audit function has the necessary resources and access to information to perform its role;
- Review the independence of the internal audit function including where appropriate/applicable, appointment, evaluation, compensation, replacement or dismissal of the internal auditor;
- Provide oversight of and interact with the organization's external auditor;
- Approve or recommend to the Head of Entity or Board for approval, the appointment, retention, compensation, evaluation and, where appropriate/applicable the replacement of external auditor; and
- Receive key audit reports regarding risk management, governance and internal control and ensure senior management is taking necessary and timely corrective actions to address control weaknesses, non-compliance with policies, laws and regulations, and other issues identified by auditors and other control functions.

4.3. Senior Management

Senior management leads the execution of the MDA's strategy and is responsible and accountable to the Head of Entity or Board for its sound and prudent day-to-day management. Managers at this level are therefore responsible for designing, implementing, and executing ERM to ensure the achievement of strategy and business objectives. Senior management sets the "tone at the top", encouraging open and transparent discussion of risk as part of the values, behaviours, and norms that define the culture of the entity. Under the direction and oversight of the Head of Entity or Board, senior management ensures that the organization's activities are consistent with the strategic objectives and risk appetite approved by the Head of Entity or Board. The function leads the development and implementation of the ERM Framework, including the entity's risk identification, assessment and reporting processes; training and sensitization; and the establishment of the risk culture, risk appetite, risk tolerance levels and limits to be approved by the Head of Entity or Board. Their risk management responsibilities include:

- Promote effective risk management, which encourages informed and intelligent risk-taking, by setting a strong 'tone at the top'. Support open discussion about uncertainties, encourage employees to express concerns and maintain processes to elevate concerns to the appropriate levels;
- Determine the entities' strategic approach to risk and set the risk appetite, balancing the need for innovation with sound resource management;
- Establish objectives that consider the entities' context, resources, capabilities and risk appetite into account. Ensure that planned activities are consistent with these objectives and risk appetite;

- Design and implement a proportionate risk management and internal control system in accordance with approved policies. Delegate responsibility to various levels of management and embed a risk culture where employees at every level manage risk as an intrinsic part of their responsibilities;
- Determine the KPIs and reporting metrics (type and frequency) needed to monitor ERM performance, including levels of risk exposure;
- Monitor the performance of the ERM process across the organization including the level of risk exposure and control effectiveness. Ensure that the risk exposure does not exceed risk appetite;
- Ensure that the approval process for all programmes, activities, processes and systems includes an assessment of risks;
- Identify changes to risks or emerging risks and promptly bring these to the attention of the Head of Entity or Board where appropriate. Act on risk information in a timely manner; and
- Collaborate with the ERM Function and report to the Head of Entity or Board on risk management and internal control processes;
 - risk profile of the entity, including directions of key risks;
 - changes in strategy and risk appetite;
 - breaches to risk limits or compliance rules;
 - operation of internal control, including notable failures; and
 - new and emerging risks e.g. from legal or regulatory concerns.

4.4. *General Staff*

- Act as risk champions in their area of work;
- Support the identification and management of risks within the organization;
- Manage risks related to their area of work, within their delegated authority;
- Perform within the agreed risk appetite and risk limits;
- Balance risk avoidance with seizing opportunities; and
- Escalate risk management issues and concerns to the ERM Function or senior management.

4.5. *Middle Management / Head of Units (First Line of Defence)*

Middle management / Heads of Units represent the First Line of Defence for conducting sound risk management. As the principal owners of risk in their areas, they set objectives, establish acceptable variation in performance, train personnel and reinforce risk responses. They implement and execute the day-to-day activities to manage performance, take risks within the assigned limits of the entities' risk appetite and are responsible and accountable for the ongoing management of risks. This includes identifying, assessing, monitoring, managing, and reporting such exposures, taking into account the GoJ's policies, procedures and controls. Their specific responsibilities are to:

- Establish and maintain a risk culture within departments / teams that this is consistent with the 'tone at the top'. Support open discussion about uncertainties, encourage employees to express concerns and maintain processes to capture these concerns;
- Identify and assess risks to the achievement of objectives in line with documented risk practices;
- Design and implement effective controls where the residual risk level falls outside the agreed risk appetite, including training personnel on required risk responses;
- Own and manage risks and controls on a day-to-day basis, by monitoring ongoing risk exposure through continual horizon scanning and monitoring of effectiveness of controls;
- Identify, monitor and escalate high priority issues, including emerging risks, to senior management; and
- Comment on risk management policies, standards and processes that are not consistent with the entity's needs.

4.6. Risk Management Function (Second Line of Defence)

This risk management function represents the Second Line of Defence and complements risk activities through its monitoring and reporting responsibilities. The risk management function must be sufficiently independent of the business - this independence is an essential component of an effective risk management function. It must have access to all programmes and functional lines that have the potential to generate material risk to the organization.

The risk management function should have the organizational stature, authority and necessary skills to oversee the public entity's risk management activities and to execute its responsibilities. The risk management function must not, under any circumstances, assume responsibility for managing any risks other than those directly relating to the core activities of its function.

The Risk Management Function's role is to assist management in performing their risk management duties, and to provide guidance and support. They should not make decisions relating to the organization's risks, or the actions taken to treat them. They should:

- Publicize and champion ERM throughout the organization and be the first point of contact with regards to the GoJ's risk management policy and guidelines;
- Develop and distribute tools, techniques and methodologies to assist the organization in optimizing its risk management processes. Support senior management in integrating risk management practices into their operational planning process;
- Provide guidance and training on the ERM process and share best practice and lessons learned;
- Facilitate risk management activities within the organization e.g. distributing risk questionnaires, running risk workshops;
- Quality review risk outputs e.g. risk registers;

- Receive reports on risk and control activities from risk owners, update the risk register accordingly and chase outstanding actions;
- Periodically review the organization's strategic risk register, checking that it reflects the current risk position;
- Collate and analyze risk data in order to identify trends, accumulated material risks and emerging risks. Prepare reports for the Risk Management Committee and senior management;
- Analyze the level of risk exposure against risk appetite and, where the two are not aligned, escalate to the Risk Management Committee and senior management;
- Consider the appropriateness of the entity's risk appetite and make recommendations to the Risk Committee and senior management in this regard;
- Periodically review the design and operation of ERM and, where these do not meet the organization's needs, make recommendations to the Risk Management Committee and senior management; and
- Participate in GoJ-wide risk management discussions and ensure a consistent approach to risk management by sharing knowledge and best practices.

4.7. Assurance Function: Internal Audit (Third Line of Defence)

The Third Line of Defence, the internal audit function performs audits or reviews of ERM practices (amongst other activities), identifying issues and improvement opportunities as well as making recommendations. The internal audit function provides independent assurance to the Head of Entity/ Board, Audit Committee and senior management on the quality and effectiveness of the MDA's/PBs internal control, risk management and governance systems and processes. The audit function assists in protecting the MDAs, public bodies and their reputation.

4.8. External Auditors and Regulators

Groups such as external auditors and regulators will play an important role regarding the organization's overall governance and control structure. External auditors provide senior management, the Board and Head of Entity with an independent and objective view that can contribute to an entity's achievement of its strategy and objectives. External auditors may also provide important observations and assessments of the organization's controls over financial reporting and related risks. Similarly, regulators establish requirements often intended to strengthen governance and control, and they actively review and report on the organizations they regulate. External auditors and regulators, while they contribute valuable information, should not be considered as substitutes for the internal lines of defence as it is the organization's responsibility to manage its risks.

5. Policy Maintenance and Review

The governing body for ERM being the Ministry of Finance is responsible for reviewing the ERM Policy every three (3) years in consultation with MDAs and public bodies. However, if there are changes to the international standards the Policy shall be reviewed and updated more frequently (see Version Control at the end). It shall also be reviewed and updated more frequently if there is a major change to the MDA's or public body's risk management and internal control systems caused by a change in function, an election, a change in strategy, market conditions or any other major events that may impact delivery of the organization's mission.

ERM Governance Structure

The Head of Entity or Board of Directors

Task	Frequency	Documentation
Oversee development of and approve the MDAs' objectives and strategy, and monitor their implementation.	Annually and as necessary in year.	Strategic and business plans.
Play a lead role in establishing the GoJ's culture and values.	On-going.	Reflected in policies and guidance used within the GoJ and MDA.
Establish, with senior management, the MDA's risk appetite.	Annual review once established.	Risk appetite statements for staff reference.
Approve and oversee the MDA's risk management policy and governance framework, with periodic reviews to ensure its continuing relevance.	Annually or when a significant change occurs.	Revised policy and framework.
Monitor the MDA's risk exposure and whether or not this is consistent with the established risk appetite.	At least half yearly.	Risk reports produced by the Risk Management Function and response to recommendations.
Review reports from Risk Management Function / Committee and discuss, request and/or approve actions.	Three or four times a year.	Reports from reporting bodies and relevant responses.
Engage with management to understand how risks relevant to the MDAs are properly identified and managed.	At least annually.	Discussion and review of risk registers and strategic and business plans.

Risk Management Committee

Task	Frequency	Documentation
Keep under review the design of the ERM framework and make recommendations for any changes.	At least annually.	Report from the Risk Management Function, responding to recommendations.
Review, challenge and advise the Board / Head of Entity on the risk appetite statements and any instances where exposure and appetite are not aligned.	At least annually and where exposure exceeds appetite.	Risk appetite statement revisions. Reports from the Risk Management Function, responding to recommendations.
Foster a strong, risk-aware culture.	At every opportunity and at every meeting.	Reports on risk management activities, prepared by the Risk Management Function and risk owners highlighting changes in risk exposures and actions to manage risk.
Supervise and support the Risk Management Function.	At every opportunity.	Receiving and responding to reports.

Audit Committee

Task	Frequency	Documentation
Foster a strong, risk-aware culture.	At every opportunity and at every meeting.	Open and transparent discussion of risk with updated risk registers.
Receive audit reports on risk management and ensure senior management take the necessary corrective actions.	Annually.	Meeting minutes, response to audit reports and audit follow up reports.

Senior management

Task	Frequency	Documentation
Set the “tone at the top”, including values, behaviours and norms that are consistent with the agreed risk appetite and risk framework.	At every opportunity.	None.
Design and implement the risk management framework to enable achievement of strategic and business objectives.	As necessary, but should be reviewed annually as a minimum.	Revised Policy, Guidelines and risk documentation.
Determine the strategic approach to risk and set the risk appetite.	Annually.	Risk appetite statements to be agreed with the Audit and/or Risk Committee and Head of Entity/Board.
Monitor the performance of ERM across the MDA, including setting risk performance indicators.	At least every six months but more frequently until risk performance is established.	Reports from the Risk Committee, and/or the Risk Management Function resulting in directions to management.
Provide leadership and direction with regards to risk management.	At every opportunity.	None.

Middle management/Heads of Units

Task	Frequency	Documentation
Establish and maintain a risk culture within departments and teams. Support open discussion about uncertainties.	At every opportunity.	No formal documentation, but likely to be in team meeting agendas and other staff discussions.
Identify, assess, own and manage risks by implementing effective controls.	To be determined according to need.	Revised risk registers and risk action plans to be reported to senior management, the Risk and/or Audit Committee and others as necessary.
Contribute to risk management arrangements by commenting on policies and procedures and supporting their staff	As necessary, but should be reviewed annually	Comments to the Risk Management Committee/Ministry of Finance Risk Policy Division in a bid to influence

Task	Frequency	Documentation
in delivering them.	as a minimum.	revision of Policy and/or other risk.
Identify, monitor and escalate high priority issues to senior management.	As necessary.	Revised risk registers reported to senior management.

Staff

Task	Frequency	Documentation
Act as risk champions in their area of work.	At all times.	Potentially revised risk registers through highlighting potential risks to the office responsible for risk (senior management/risk function)
Support the identification and management of risks within the MDA.	At all times.	
Manage risks related to their area of work, within their delegated authority.	At all times	
Escalate risk management issues and concerns to the ERM Function or senior management.	At all times	

Risk Management Function

Task	Frequency	Documentation
Publicise and champion ERM throughout the MDA and be the first point of contact for queries.	At all times.	Guidance notes, updated intranet, improved risk registers, etc.
Develop and distribute tools, techniques and methodologies.	At all times.	Tools, guidance, methodologies.
Provide guidance and training on the ERM process and share best practices.	At all times.	Guidance notes, updated intranet, training materials.
Facilitate risk management activities.	Following a set programme.	Output from activities, e.g. improved risk registers.
Review and challenge risk registers, keeping them up to date and identifying trends.	Following a set programme.	Reports to the Risk Management Committee.
Review and challenge of risk appetites to check their continuing relevance and application.	At least annually.	
Review of the design and operation of ERM.	At least every two years.	

Internal audit

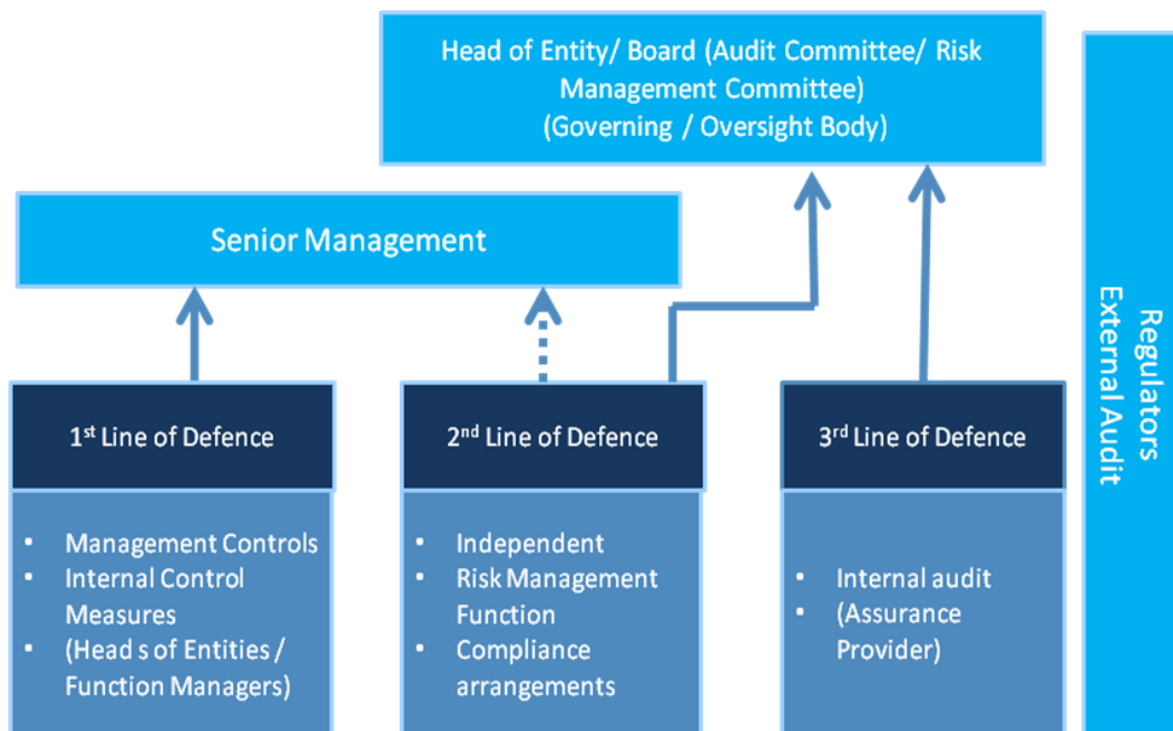
Task	Frequency	Documentation
Assess the effectiveness and efficiency of the risk governance framework and its application.	Annually.	Audit report for management action and noting by the Audit and Risk Committees, annual audit opinion.
Provide assurance on risk	Annually.	Audit report for management

Task	Frequency	Documentation
management arrangements.		action and noting by the Audit and Risk Committees.
Validate risk information and risk reporting.	Annually as part of the assurance audit.	Audit report for management action and noting by the Audit and Risk Committees.

Three Lines of Defence Model

The GoJ's Risk Governance Structure set out in Section 5 follows the principles of the Three Lines of Defence Model, a widely used model which includes well defined roles and responsibilities for risk management and control activities. This model distinguishes between functions that own and manage risks, functions that oversee risks and functions that provide independent assurance.

Figure 4. Three Lines of Defence Risk Governance Model



The Three Lines of Defence Model includes:

1. First Line of Defence

The first line of defence consists of management and staff who are responsible for identifying and managing risks to the achievement of objectives. They are risk owners and are responsible for the design and execution of controls to identify and respond to any risks with residual exposure outside of the entity's risk appetite.

2. Second Line of Defence

The risk management function is independent of the first line of defence. It is an oversight function that co-ordinates and facilitates the effectiveness and integrity of the ERM Framework. The second line provides the necessary framework, tools and support to the first

line. It monitors the implementation of the risk management framework to ensure consistent and effective implementation and provides consolidated and analysed risk information to the Board, Risk Management Committee and senior management. It challenges and advises where the risk exposure is not within approved limits.

3. **Third Line of Defence**

This line is independent from the first and second lines of defence. It provides independent assurance and challenge across all programmes and functions in respect of the integrity and effectiveness of the Framework. This line is not a management function.

The Head of Entity or Board and Senior Management

Although the Head of Entity or Board and executive management are not considered to be part of one of the three lines, they have integral roles in the ERM Governance Structure. They are responsible for providing risk oversight of ERM, and senior management is accountable for the selection, development, and evaluation of the system of internal control with oversight by the Head of Entity or Board.

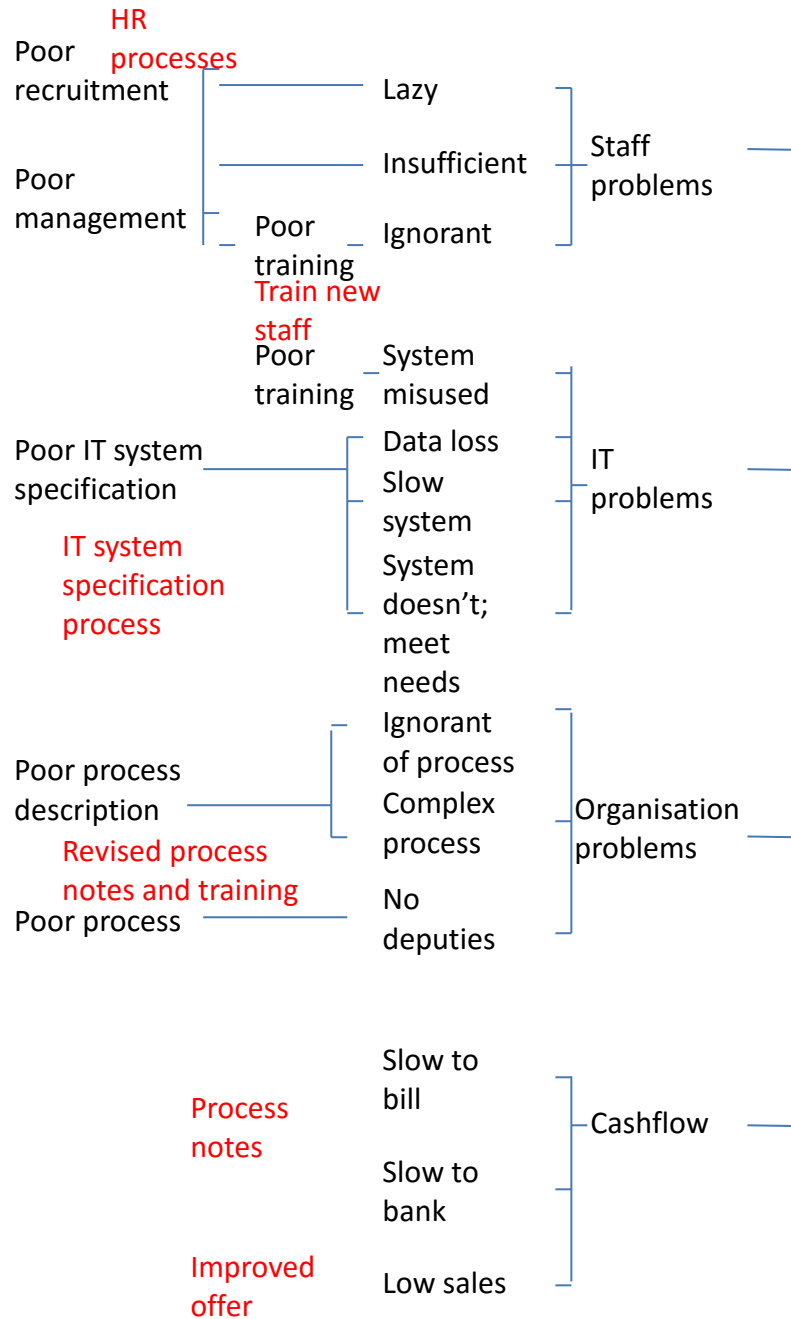
Bow Tie

A risk Bow Tie is a diagrammatic representation of each risk, showing the causes, consequences and controls and their interrelation. There is a sample Bow Tie on the next page. It may require a few attempts to get this right and to correctly identify the risk itself as opposed to the causes and consequences, but this is a useful part of the process of understanding a risk. The process is broadly as follows (it may be easier to jump back and forth between steps):

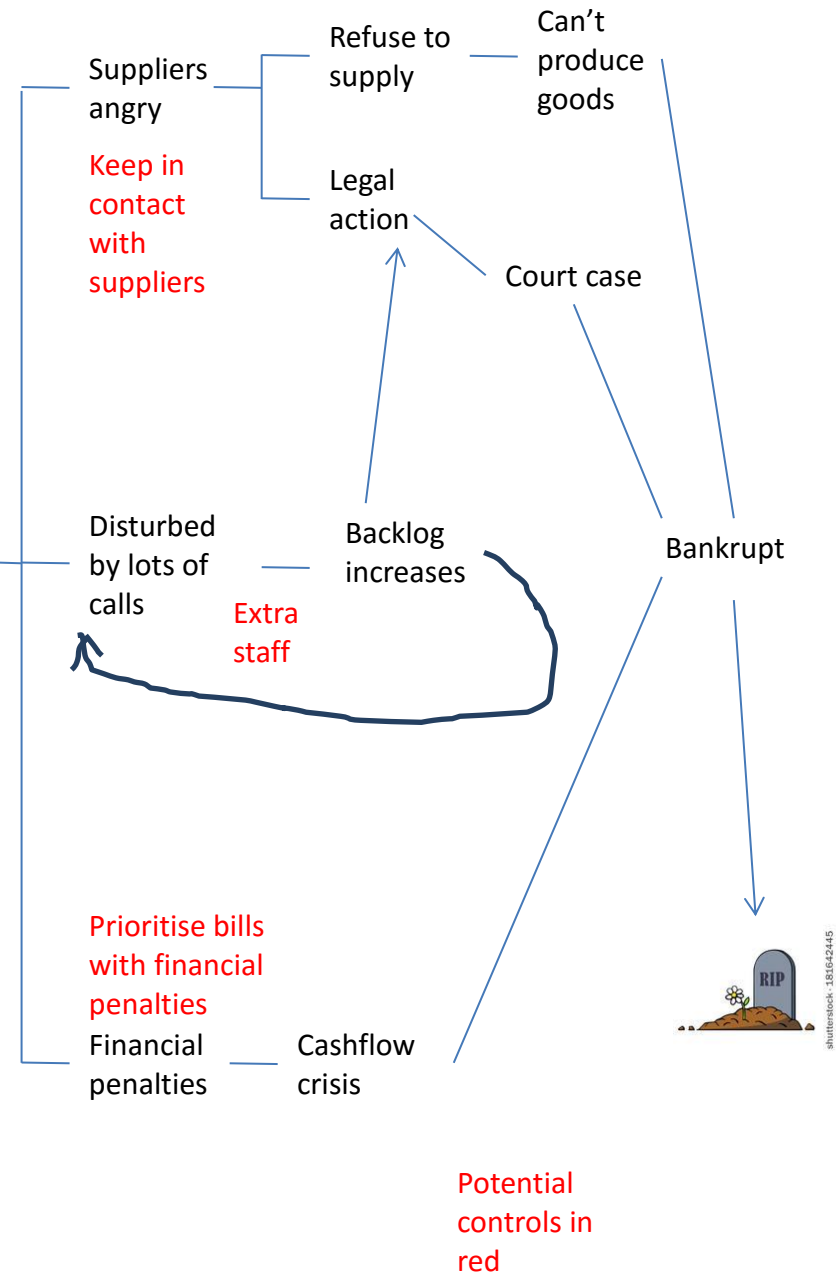
1. Identify a key risk for the centre of the diagram. As the Bow Tie is developed, it may be that it becomes clear that this original risk is in fact a cause or consequence.
2. Think about the consequences (to the right of the Bow Tie) should that risk occur and list them out, showing which consequences are linked to others and which are consequential on others. The general process is from minor consequences to more serious consequences to complete disaster, but this may not necessarily be the case. Finish when there are no more ideas, or these ideas are extreme or the consequences are beyond the GoJ's control.
3. Think about the causes (to the left of the Bow Tie) of the risk. You should consider what might be the immediate trigger but also why did that trigger happen and so on. The recommendation is that you ask "why?" five times (although this may be too often or too few iterations). Finish when you run out of ideas or the causes are clearly beyond the control of the GoJ. As for consequences, link common causes and show their hierarchy.
4. Start identifying the controls (in red in the Bow Tie) that could manage the causes and consequences that you have listed. Ideally you want to control your root causes (those to the far left of the Bow Tie) and immediate consequences (those closest to the middle of the Bow Tie) but if you cannot control at this level then look for other places to include controls. Remember that there may be some causes and consequences that are uncontrollable.

When you have completed this process, you will have captured the "story" of the risk in a way that clearly describes it.

Causes



Consequences



Risk identification form

<p>Title of risk/general theme of risk</p> <p>Link to strategy/objectives</p>		<p>Current risk score: L = Likely I = Impact</p>	
<p>Causes, ideally grouped to identify common themes and the immediate and more remote causes</p>		<p>Consequences, ideally grouped to identify common themes and the immediate and more remote consequences</p>	
<p>Current controls</p>	<p>Assurance</p>	<p>Further actions/who/when</p>	<p>Assurance</p>
			<p>Target risk score: L = Likely I = Impact</p>

Risk typology

Category	Description
Political	Risks relating to the political process, that may impact on decisions that need to be made at the Government-wide level
Economic	Risks relating to financial matters, for example anything relating to cash collection, budget management, grant funding, etc.
Sociological	Risks relating to sociological or demographic change, for example the risk resulting from more children being born or an ageing population
Technological	Risks relating to the use of or implementation of technology, for example risks associated with providing more services on line
Legal	Risk that, should they occur, would result in legal consequences and risks relating to implementing new laws
Environmental	Risks that, should they occur, would result in environmental harm in some way or risks relating to activities that affect the environment, for example flood relief, road building, etc.
Ethical	Risks relating to the behaviours, culture and values of employees, for example the risk of employee fraud, bribery or corruption
Assets	Risks relating to the physical assets of the GoJ, for example the risks associated with buying, selling or owning property, the risk of damage to property, etc.
People	Risks associated with having employees, for example recruitment and retention risks. While this is closely linked to ethical risks, it is more about people as an asset of the GoJ and not so much about what they actually do
Reputation	Risks that, should they occur, would lead to damage to the reputation of the GoJ. Almost any risk has the potential to lead to reputation damage so this category should only be used where the major concern is to manage the GoJ's reputation
Information	Risks relating to the management of information, for example data loss, theft or corruption, misuse of data or publishing incorrect information
Continuity of operations	Risks that, should they occur, would make it difficult or impossible for the GoJ to continue with normal operations. This could be as a consequence of natural disasters or for other reasons, for example power outage. It is likely that these risks could also fall into another category so only use this category when the major harm is due to the GoJ's inability to continue to operate

Impact and likelihood scoring

Impact: To determine the impact of an event, should it occur, the possible types of impact should be kept in mind. Descriptors have been given for each type of impact; rates range from minor (1) to catastrophic (4). These should be used as guidance to help with the assessment of impact scores.

	Minor (1)	Moderate (2)	Major (3)	Catastrophic (4)
Objective delivery Failure to deliver planned objectives	Cannot deliver part of a significant objective Compromise on quality/quantity affecting more than one significant objective	Cannot deliver most of a significant objective or parts of more than one objective Compromise on quality/quantity seriously affecting more than one significant objective	Cannot deliver a significant objective or parts of most objectives Serious compromise on quality/quantity of most significant objectives	Fail to deliver most objectives Serious compromise on quality/quantity of all objectives
Reputation Lack of/too much visibility, dissemination of incorrect information, information leaks, unethical behaviour, etc.	Limited damage to reputation Minor one-off negative local publicity or visible dissatisfaction by local stakeholder groups	Some damaging negative publicity Of national interest for a few days	Negative publicity or damage to reputation resulting in ministerial inquiry and damage to public confidence Minor international interest	Significant and sustained negative publicity or damage to reputation resulting in senior staff resignation/removals, inquires, significant damage in public confidence Sustained international interest
Financial cost ¹⁵ Excess costs, shortfalls in income, procurement issues, financial losses, etc.	Manageable within current budgets	Will require changes to planned budgets to manage and delays to planned activities	Planned budgets cannot be met and planned activities will have to be cancelled	Emergency funding will be needed to ensure that basic services can continue to be delivered

¹⁵ Parameters need to be set dependent on each entity to which this is applied

Human resources Lack of motivation, frustration, conflicts, recruitment and retention, dismissals, etc.	Low level dissatisfaction in some but not all areas, turnover at expected levels, slight downturn in applicants for jobs	General low-level dissatisfaction, increased grievances, turnover increased, noticeable reduction in applicants for vacancies	Short-term strikes, increased short-term sick levels, turnover difficult to manager, few and low-quality applicants for jobs	All out strike Work to rule Cannot recruit
Ability to operate Breakdown of business delivery systems (IT, financial, etc.)	Minor glitches in systems that delay work but not for long Reducing level of assurance given by internal audit	System problems cause noticeable delays in delivery of activities Internal audit routinely giving low assurance	System problems resulting in failure to deliver important objectives Internal audit routinely giving no assurance	System problems resulting in failure to deliver majority of important objectives Internal audit routinely giving no assurance

Likelihood scoring is based on the knowledge and actual experience of those assigning the score. In assessing likelihood, it is important to consider the nature of the risk. Risks are assessed on the probability of future occurrence; how likely is the risk to occur over a given period of time? How frequently has it occurred? Do not rely entirely on the frequency with which events have happened in the past but use this as an indicator only.

It should be noted that, in assessing risk, the likelihood of a particular risk materialising depends upon the effectiveness of existing controls; consideration should be given to the coverage and robustness of existing controls in place, with evidence available to support this assessment.

The assessment of likelihood of a risk occurring is assigned a number from 1 (unlikely) to 4 (almost certain) over a timeframe of three years, to tie in with the strategic planning cycle

Highly unlikely (1)	Unlikely (2)	Likely (3)	Highly likely (4)
This may happen once in the next three years but it is unlikely to do so It hasn't happened in recent memory	This is likely to happen at least once in the next three years, but not more often than that It has happened once in the last three years	This is likely to happen more than once in the next three years It has happened a few times in the last three years	This is likely to happen several times in the next three years It has happened many times in the past

Risk map

The combined effect of the risk impact and likelihood defines the level of risk exposure and is plotted on a risk map to give the overall picture of risks facing the organisation. Each risk is assessed according to its likelihood and impact, using the tables in Appendix 5. The number in the cell in which it is placed indicates the priority given to that risk. Note that the scoring mechanism weights towards impact.

Impact	Catastrophic (4)	10	13	15	16
	Major (3)	6	9	12	14
	Moderate (2)	3	5	8	11
	Minor (1)	1	2	4	7
		Highly unlikely (1)	Unlikely (2)	Likely (3)	Almost certain (4)
		Likelihood			

Depending on the level of exposure, different actions should be undertaken:

1-7 – Low – Green

Low risk exposure: the risk represents no immediate threat or impact and does not require any further action but should be monitored for changes.

8-11 – Medium – Amber

Medium risk exposure: the risk has the potential to cause harm and could become a high risk. Cost-effective actions should be taken to reduce the level of risk to green and the risk should be routinely monitored for changes that could move it into the red zone.

12-16 – High - Red

High risk exposure: the risk requires active management and is currently beyond the Government of Jamaica's risk appetite. It poses an immediate threat and its impact could be significant. Practical actions should be put in place to manage this to amber and, in the meantime, the risk should be monitored frequently to identify any changes that could make it more likely to occur.

Appendix 8

Sample risk register

Risk no	Associated objective	Risk title and owner	Causes (why?)	Consequences (so what?)	Current controls and owner	Assurance on current controls	Residual risk score ¹⁶		Further actions	Who	When	Assurance on future actions	Target risk score ¹⁷	
							L	I					L	I
Title/grouping/category for risks that follow														
Unique number for each risk to provide an audit trail	Which strategic objective(s) this risk could impact	A brief title for the risk and a senior manager to take responsibility	Bulleted list of underlying causes for the risk, ideally in hierarchical order	Bulleted list of consequences should the risk occur, ideally in hierarchical order	What is already been done to manage this risk and who is responsible for that control	How do we know that this control is working? Broken down into three lines of defence			If this risk is outside our risk appetite what more are we going to do about it? NFA if within appetite			How do we know that these actions are being delivered? Broken down into three lines of defence		

¹⁶ Residual risk score is the score with current controls in place and reflects the efficacy of those controls

¹⁷ Target risk score is what it is anticipated can be achieved when all planned actions have been fully implemented

Risk appetite measures

Risk levels and description	Minimal	Cautious	Open	Seek
Key elements	As little risk as reasonably possible	Prefer safe delivery options	Consider all potential options	Eager to be innovative
Financial (lower of value or % loss) VFM	Very limited financial loss - Up to 2% of total project cost VfM (focusing on economy) is primary concern	Some limited financial loss - Between 2-5% of total project cost Consider benefits and constraints beyond price	Will invest and risk losing - Between 5-7% of total project cost/ potential returns Value and benefits considered, not just cheapest price	Invest and risk losing - Between 7-10% of total project cost/best possible return Resources allocated without firm guarantee of return
Acceptability Exposure to litigation	Plans not at all controversial No risk of litigation	Likely to be minimum controversy Win over doubters easily Litigation over trivial matters only and easily won	Some controversy expected Likely to create lingering but low-level dissension Potential for significant litigation that could result in financial loss	Plans are controversial Expect continuing dissension Litigation likely and may result in significant loss
Innovation, Quality	Innovations avoided unless essential or commonplace Decision making by senior management Essential systems or technology development only	Prefer status quo and avoid innovation Decision making generally by senior management Limited systems or technology development	Innovation supported Non-critical decision making devolved Routine systems or technology development	Innovation pursued High levels of devolved authority New technologies seen as key enabler of operational delivery
Reputation	No chance for significant repercussions Avoid exposure to attention	Little chance of significant repercussions Mitigation in place for undue interest	Will expose to scrutiny and interest Prospective management of reputation	Will bring sustained scrutiny New ideas have potential to enhance reputation
Impact on human resource capacity	Insignificant capacity impairment	Limited impact on business processes	Will undermine the Ministry's ability to deliver services on a timely basis	Could cripple the MDAs that rely on the Ministry for financial resources and policy direction
Appetite	Low	Moderate	High	Significant

Version control

Version number	Date	Changes made	By whom