`

GOVERNMENT OF JAMAICA

ENTERPRISE RISK MANAGEMENT GUIDELINES

Version 1.0

Version control

Version number	Date	Changes made	By whom
1.0	November 1, 2021	First Issue	MoFPS, PXPC

Contents

1. Managing Risk within the Government of Jamaica

Private or public, no organisation 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 the 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 within the Central Government and other government entities that are partially or fully funded by the Consolidated Fund referred to as Ministries, Departments and Agencies (MDAs), in this guideline. It also serves as a guide to self-financing public entities.

It gives a practical, structured and pragmatic approach to risk identification and management that will work alongside the Entity's current management activities and not be overly burdensome and bureaucratic.

1.1. Why Manage Risk?

The risk policy states that risk management is recognised 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 realising opportunities. Ultimately, risk management is good management. By seeking to identify, prioritise 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.

1.2. Defining Enterprise Risk and Risk Management

Good risk management supports you in being proactive in recognising 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.[1]
Risk management	A process to identify, assess, manage and control potential events or situation to provide reasonable assurance regarding the achievement of the organization's objectives.[2]
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 realising value.[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:

a) 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

b) 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

c) 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

[1] Institute of Internal Auditors: International Practices Framework

[2] Ibid

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

your risks, seek to understand them and manage them in an appropriate fashion, taking value for money into account

d) 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

e) Do not take risk management as an exact science: it is based on professional judgement and will support good management practices.

2. Operationalising ERM in Government

The whole of government approach to an ERM requires the creation of a policy as well as clear guidelines on what and how the process should be carried out. It also allows for standardization for comparison and across government analysis of strategies that inform business decisions and create prudent financial management of resources. Therefore, this guideline includes tools and techniques on how to implement and maintain an effective ERM process. The document outlines the following steps in developing and maintaining an effective ERM process:

a) Assessing and modelling the entity's ERM Maturity. It is important to establish the level at which the entity is preserving, assessing, and addressing risks within the entity. An assessment of the risk maturity level will allow for the development of an adoption/maturity strategy for the entity.

b) Risk adoption/maturity process. The ERM process takes time to implement and even more time to have a substantial impact on the financial management and the operations of an entity. However, the process must start to be able to climb the ERM maturity hierarchy. It starts with having a plan of action; this plan of action should be outlined in the ERM framework.

c) Establishment of an ERM Framework. The aim of a risk management framework is to set the environment, governance and strategy for clear directives on how to operationalize the risk management process within the organisation. The Risk Management Framework must also give the staff sufficient information to know the perimeter in which to function, clear roles and responsibilities, reporting protocols and the respective authority to act. It also allows for an effective mechanism to link key performance indicators (KPI) with risk management.

d) Assessing and managing risk. The aim of this component is to embed risk management in the decision-making process to ensure that personnel throughout the GoJ entity are working to achieve its objectives. It involves risk assessment, mitigation strategy, reporting and monitoring of key risk indicators (KRI).

2.1. Risk Management Maturity Model

The level of adoption of the risk management principles needs to be assessed to determine the level of risk awareness within the entity and its infusion into the operations and decision-making process. There are varying tools that can be used to assess the entity's risk awareness and risk management process. A risk maturity model is one method that can be used to ascertain the level of risk awareness, culture and management process within the entity and is being recommended as the tool to be used by GOJ entities. Each entity must therefore establish its risk maturity level to ensure a strategy is crafted in the Risk Framework to improve the risk management status of the entity. The aim is to include in the risk framework, targeted strategies to address the weaknesses or nuisances identified in the maturity assessment process.

The table below depicts a Risk Maturity template that may be used. There are other Maturity Models/templates that are available and can be used, once it follows similar tenets to the model shown below.

The four categories that are used within this assessment are:

Process – Use of Standards, Tools and Techniques	**Culture** – Risk Management activities undertaken
Adoption – knowledge of Risk Management Discipline	**Visibility and Control** – Awareness of benefits and value

These four main areas cover the ISO principles and create a guide for the Risk Management Framework within the entity.

Risk Management Adoption Maturity

	Definition	Learner	Developer	Performer	Contender	World Class
Parameters of Implementation	**Process** – Use of Standards, Tools and Techniques	No use of Standards, Tools and Techniques	Aware of Techniques but no formal application of Standards	Use of Standards and Risk Management Tools	Regular use of Standards and Risk Management Tools	Sound understanding of Standards, good use of Tools to support the process
	Adoption - knowledge of Risk Management Discipline	Little Knowledge of Risk Management Disciplines	Aware of Risk Management, not clear on how it may benefit the organization	Understanding of Risk Management across some parts of the organization	Sound Knowledge of Risk Management and its value to the organization	High degree of organizational awareness and knowledge of Risk Management
	Culture – Risk Management activities undertaken	No formal management activities undertaken	Conduct some risk management activities (ad hoc) insufficient resources	Have Risk Management Framework and carry out Risk Management when time permits	Formal Risk Management programme in place	Risk Management embedded in the organization and decision making
	Visibility and Control – Awareness of benefits and value	Unsure how Risk Management may benefit the organization	Aware of the need to formalize Risk Management. Not clear on broader organizational benefits	Aware of the benefit that Risk Management brings to the organization	Aware of the benefits of Risk Management with deployment across the organization	Risk Management incorporated into business planning and strategic thinking
		1	2	3	4	5

Risk Management Maturity Model 2-1

Each level within this risk maturity model can assist in identifying the position at which the entity is operating. It also gives an indication of the strategies required to move the entity to the next level.

The task requires management to conduct behavioural and cultural assessment of the staff, management's approach and action to risks affecting the entity. The need to use a tool to determine the risk management maturity level becomes important as it offers a reliable mean for the conclusion reached. The tool should also identify mechanisms to address each issue identified; this should be included in the Framework. Therefore, it will be expected that each entity will assess its risk management maturity and at the same time, address the principles set out in the ISO 31000 architecture.

There are varying methods/tools that can be used to ascertain the level at which the entity is operating. These assessments can be done using, for example:

e) Survey/questionnaire

f) Focus Group by staff levels

g) Gap analysis exercise

Regardless of the tool or methodology used, the aim is to ensure that a fair and accurate assessment is done so that the Risk Framework is informed by credible data.

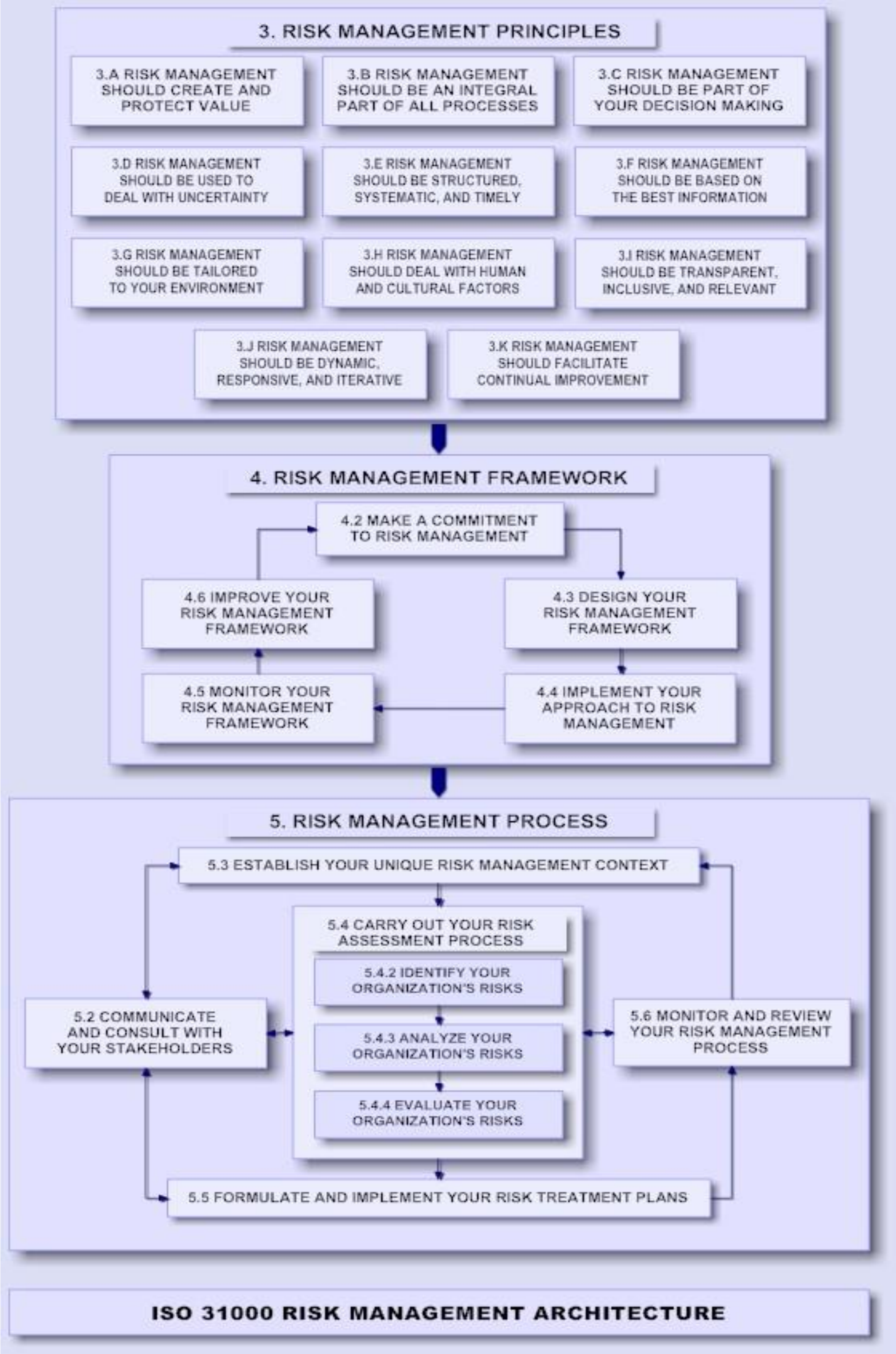
3. Enterprise Risk Management Framework in the Government of Jamaica

The risk management process starts with the establishment of a risk framework which sets principles by which the organisation will operate. The design and implementation of a risk management framework within government entities, should consider their varying needs, objectives, context (specific practices employed), structure, operations, processes, functions, projects, products, services, and assets (PECB, see **Appendix 1 – Glossary**).

To craft a risk framework for the entity, knowledge of the risk management maturity level is required, see previous section (2.1). Therefore, each entity needs to determine the risk level of the entity by categories and outline an implementation strategy to move the entity to the next level in its risk maturity journey. However, to do this assessment, an understanding of the risk management integration, with risk management principles and practice is required.

In 2018, the Cabinet approved the adoption of the ISO 31000 Risk Management Framework. The ISO 31000 standard sets the foundation for instituting a successful risk management process. The ISO Standard first outlines the need to establish a risk tone within the organisation by way of the principles that it sets out; (see figure 1-1 below for details). The principles embody the manifesto for a risk framework. Therefore, these guiding principles must be adopted by all government entities and should be clearly stated within the risk management framework.

ISO 31000 Relationship between Risk Management Principles, Framework and Process


3. RISK MANAGEMENT PRINCIPLES
3.A RISK MANAGEMENT SHOULD CREATE AND PROTECT VALUE
3.B RISK MANAGEMENT SHOULD BE AN INTEGRAL PART OF ALL PROCESSES
3.C RISK MANAGEMENT SHOULD BE PART OF YOUR DECISION MAKING
3.D RISK MANAGEMENT SHOULD BE USED TO DEAL WITH UNCERTAINTY
3.E RISK MANAGEMENT SHOULD BE STRUCTURED, SYSTEMATIC, AND TIMELY
3.F RISK MANAGEMENT SHOULD BE BASED ON THE BEST INFORMATION
3.G RISK MANAGEMENT SHOULD BE TAILORED TO YOUR ENVIRONMENT
3.H RISK MANAGEMENT SHOULD DEAL WITH HUMAN AND CULTURAL FACTORS
3.I RISK MANAGEMENT SHOULD BE TRANSPARENT, INCLUSIVE, AND RELEVANT
3.J RISK MANAGEMENT SHOULD BE DYNAMIC, RESPONSIVE, AND ITERATIVE
3.K RISK MANAGEMENT SHOULD FACILITATE CONTINUAL IMPROVEMENT
4. RISK MANAGEMENT FRAMEWORK
4.2 MAKE A COMMITMENT TO RISK MANAGEMENT
4.3 DESIGN YOUR RISK MANAGEMENT FRAMEWORK
4.4 IMPLEMENT YOUR APPROACH TO RISK MANAGEMENT
4.5 MONITOR YOUR RISK MANAGEMENT FRAMEWORK
4.6 IMPROVE YOUR RISK MANAGEMENT FRAMEWORK
5. RISK MANAGEMENT PROCESS
5.3 ESTABLISH YOUR UNIQUE RISK MANAGEMENT CONTEXT
5.4 CARRY OUT YOUR RISK ASSESSMENT PROCESS
5.4.2 IDENTIFY YOUR ORGANIZATION'S RISKS
5.4.3 ANALYZE YOUR ORGANIZATION'S RISKS
5.4.4 EVALUATE YOUR ORGANIZATION'S RISKS
5.2 COMMUNICATE AND CONSULT WITH YOUR STAKEHOLDERS
5.6 MONITOR AND REVIEW YOUR RISK MANAGEMENT PROCESS
5.5 FORMULATE AND IMPLEMENT YOUR RISK TREATMENT PLANS
ISO 31000 RISK MANAGEMENT ARCHITECTURE

ISO 31000 Risk Management Architecture 3-1

The structure of ISO 31000 sets out the principles that help drive the successful implementation of a risk management framework. The principles outline the ingredients that will ensure there is adequacy in dealing with the threats that are being faced currently as well; it requires an assessment of other potential risks that the entity may face in the future. Importantly, the principles require that the risk management process evolve with time, that is, it should not be static. Key points from the ISO principles are outlined below:

- The principles provide key criteria for the success of the ERM process.
- It outlines the importance of the management team in ensuring that risk management is integrated into all organizational activities, starting with the governance of the organization. The tone must be established at the senior management level to allow for infusion of the risk management process throughout the entity.
- The acknowledgement that ERM is of an iterative nature, drawing on new experiences, knowledge and analysis for the revision of process, actions and controls at each stage of the process.
- The ERM process must be strategic and dynamic; that is, there must be a scheme that streamlines communication with great focus on sustaining an open systematic model that regularly exchanges feedback with external stakeholders to fit multiple needs and contexts.

After adoption of the ISO principles in the Government of Jamaica's (GOJ) context, a framework is required to be drafted and promulgated to all staff. This will allow all staff within the entity to understand their role and responsibility in the risk management process and their importance in the risk mitigation strategy.

3.1. Design of the Risk Management Framework

The ISO 31000 outlines the need for a Risk Management process that is tailored to the entity, its environment, culture, process and control framework, and is adoptive and flexible. Therefore, each government entity will be required to develop its Risk Management Framework to show how it will ensure the adoption of the Government of Jamaica Enterprise Risk Management Policy and the consideration of the ISO 31000 principles as outlined below:

- Integrated across the entity;
- Structured and comprehensive to ensure consistency of processes;
- Customized to the organization;
- Inclusive of knowledge, views and perceptions of key stakeholders;
- Dynamic in managing risks that change continually over time;

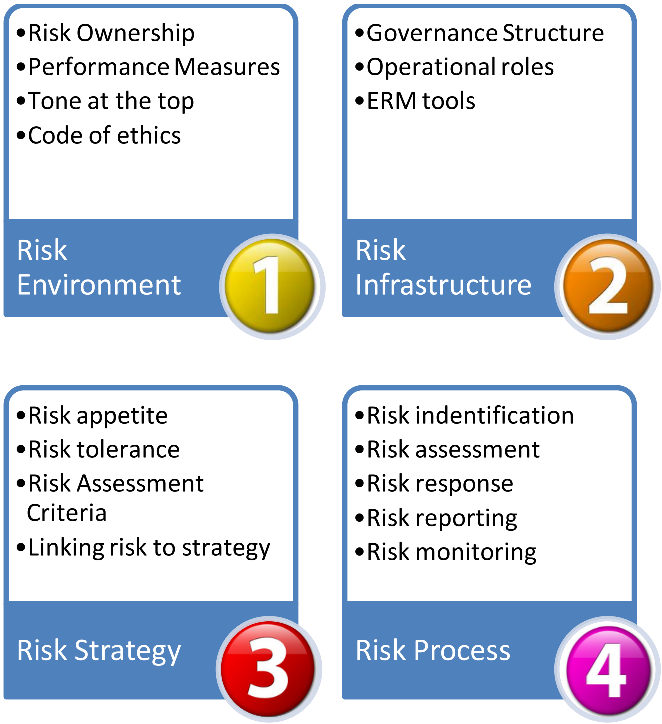
- Based on the best available information to provide timely, clear information to stakeholders;

- Developed in light of human and cultural factors that influence the management of risks; and

- A continual improvement of the risk management process.

3.2. Template for the Enterprise Risk Management Framework

The diagram below provides a guide to developing the Enterprise Risk Management Framework; these components must be included as well as management commitment. The component of the Management Commitment was dealt with in the previous segment.



- Risk Ownership
- Performance Measures
- Tone at the top
- Code of ethics

Risk Environment 1

- Governance Structure
- Operational roles
- ERM tools

Risk Infrastructure 2

- Risk appetite
- Risk tolerance
- Risk Assessment Criteria
- Linking risk to strategy

Risk Strategy 3

- Risk indentification
- Risk assessment
- Risk response
- Risk reporting
- Risk monitoring

Risk Process 4

The Framework should include, but not be restricted to the four (4) main components outlined above. The details of these components are outlined in the following chapters; however, a summary of each is as follows:

a) Risk Environment – This component sets the tone for the risk management process within the entity. It should be holistic and include the endorsement of the Head of

Entity. There should also be a clear demonstration of the entity's ethical standards. It should also outline commitment to transparent and high performance.

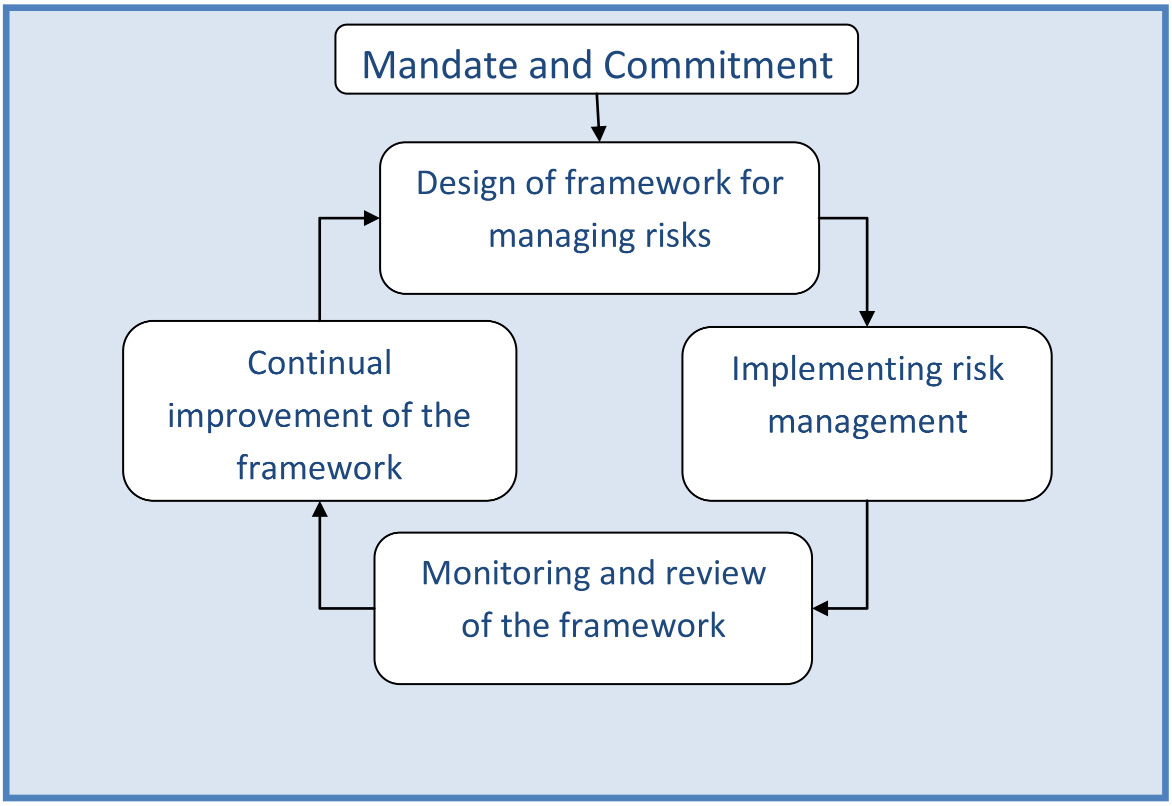
b) Risk Infrastructure – This component is critical to the success of the ERM process; it outlines the governance struture, reporting protocol and supporting tools that are needed to execute the framework. To ensure an efficient and effective risk management process, there must be clear reporting responsibilities that can be outlined in a RACI chart or some other method that would indicate each staff input in the process. There must also be tools established, such as the risk matrix, for easy accounting and management of the risk. A risk management system is also recommended to capture and analyse the data.

c) Risk Strategy – This sets the scope for the risk management process. This must be informed by the strategic objectives of the enity.

d) Risk process – outlines how the entity will carry out its risk assessment and the protocol established to account, manage and monitor the risk assessment.

3.2.1. Risk Environment

The core of the ISO 31000 Risk management architecture is the design of a Risk Management Framework. This framework must have clear mandate and commitment from the Head of entity for Central Government, or the Board in the case of Public Bodies. The mandate sets the atmosphere for the execution of the risk management process and must be shown by way of acknowledgement in the Risk Management Framework document.


Mandate and Commitment
Design of framework for managing risks
Implementing risk management
Monitoring and review of the framework
Continual improvement of the framework

ISO 31000 Risk Management Framework 1

The commitment of the Head of Entity or the Board must also be displayed in the level of priority given to the function through support and the mechanism to ensure accountability or call to action where an intolerable risk level is probable. Another important component that should be communicated in the Mandate and Commitment is the critical success factors which should be tied to staff performance. This sends a key signal from the Head of Entity or the Board to the staff, of their commitment to ensuring staff is performing their respective roles. Some of these measurable success factors/key performance indicators are:

- Senior executive driving the **ERM** process and actionable quarterly reports to the risk committee
- Targeted **ERM** culture sensitization session at all levels of the organization.
- A mechanism implemented to get feedback from stakeholders on the ERM process and the reports on actions taken to address concerns
- Clear protocol for reporting potential risk issues and transparent mechanisms in place to assess and report risks by all staff
- Rationale for decisions taken to risk committee and/or staff
- Action taken to mitigate risk once identified and/or approved
- Integration of financial and operational risks into the decision-making process

3.2.2.Risk Infrastructure

3.2.2.1. The Governance Arrangement

The Risk Policy sets out the details of roles and responsibilities, which are summarised below. Each category has specific purpose and function and supports the effective management and operations of the function.

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 internal policy and governance framework, with periodic reviews to ensure its continuing relevance.	Annually or when a significant change occurs.	Revised internal 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 Working Group and/or 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 Working Group and/or 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 Working Group, 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.

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, the Risk Working Group 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 internal policies and procedures and supporting their staff in delivering them.	As necessary but, should be reviewed annually as a minimum.	Comments to the Risk Working Group to result in revised Policy, Guidelines and risk documentation.
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 Risk Working Group and management.
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.

Task	Frequency	Documentation
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 and work with the Risk Working Group(s) to ensure risk assessment objectives are met.
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.	

Risk Working Group

Task	Frequency	Documentation
Ensures consistency in risk management arrangements.	At quarterly meetings.	Revised risk registers discussed and agreed with risk owners.
Identifies where risk management arrangements need amending.	At least annually but as necessary.	Revised internal risk documentation.
Reviews and challenges corporate, divisional and other risk registers	At quarterly meetings	Revised risk registers discussed and agreed with risk owners.
Support periodic "blank sheet" risk reviews.	At least every three years in line with the business planning cycle.	Refreshed risk registers developed in conjunction with risk owners.
Reporting on risk activities to the Risk Committee.	Half yearly as a minimum, but more often if necessary.	Reports on risk management activities, highlighting changes in risk exposures and actions to manage risk.

The main purpose of the working group is to have a small focus group to discuss, challenge and finalise risk assessments related to a specific area or varying areas. Therefore, there must be a focus and/or goals established for these working groups. This group is different from the Risk Committee, which is a requirement for the proper management of the function (see 3.3.2.1.1 below for details).

The duration of the working group is up to the management team for each entity. That is, each entity may need it at the implementation stage but may decide to dissolve after the entity has matured in its risk management process.

The composition of the group(s) must depend on the goal and the risk being assessed. These working groups should consist of internal staff however, external partners may be co-opted as the need arises.

3.2.2.1.1. The Risk Committee and its Reporting Relationship

The risk committee is important to the governance structure and provides advice to the Head of Entity/Board on the management of risks within the entity. It also has a reporting responsibility to the third line in the risk management defence system, the Internal Audit Function, on outstanding risk issues or severe risk possibility, for an assessment to be carried out.

The Terms of Reference/Charter for the Risk Committee must include the role and responsibilities outlined in the Risk Management Policy but specifically must include the following:

1. Review and prioritize the risks that have been identified to date.
2. Ensure that ownership of the risks have been assigned to the appropriate area of responsibility.
3. Oversee the key risk indicators and monitor the state of the mitigating internal controls and report to the Head of Entity/Board.
4. Approve the formation of the working group and ensure the mandate of the group(s) is established and monitored.
5. Review reports of the working group and take action where necessary.
6. Monitor and track progress of Units, responsible for dealing with accountabilities and identification of risks, and report status on individual risks to applicable Audit Committee or Board on overall risk monitoring.
7. Ensure that risk strategies are adopted on the basis of a cost-benefit analysis and that they reflect the tolerance risk level.
8. Develop and approve or recommend for approval to the Head of Entity or Board, risk management procedures and appropriate communication strategies.
9. Monitor and review training initiatives to ensure that accountability and risk management issues are being addressed.
10. Receive information on new enterprise-wide risks as they develop and prioritize them against existing risks.
11. At a minimum, report annually to the Head of Entity or Board, the top risks and the progress in dealing with them.

Other areas that must be included in the Risk Committee Charter or Terms of Reference are:

12. The composition of the committee for the portfolio Ministry. This must include at least two (2) external parties, from two of its affiliated departments that are critical to the successful achievement of the portfolio's strategic objectives; this will ensure cross-alignment of risk mitigation strategy.
13. The quorum for meetings – A quorum for each meeting should be 60% of the membership. Each entity must ensure that the committee consists of senior executive

managers or their representative. Please note, the representative must have the authority to make decisions on their behalf.

14. The frequency of meetings – It is recommended that the meeting be held quarterly, and Risk Champion must provide update on the risk management process each meeting, ***see section 4 - Risk Management Reporting***.
15. The documentation of minutes – It is important that minutes are kept, and reports provided to the Head of Entity, Board and /or Audit Committee.
16. An annual report must be presented to the Ministry with responsibility for finance on an annual basis. The report should include a summary of the risk management process for the portfolio and the key risk faced by the entity and the action being taken to mitigate the risks.

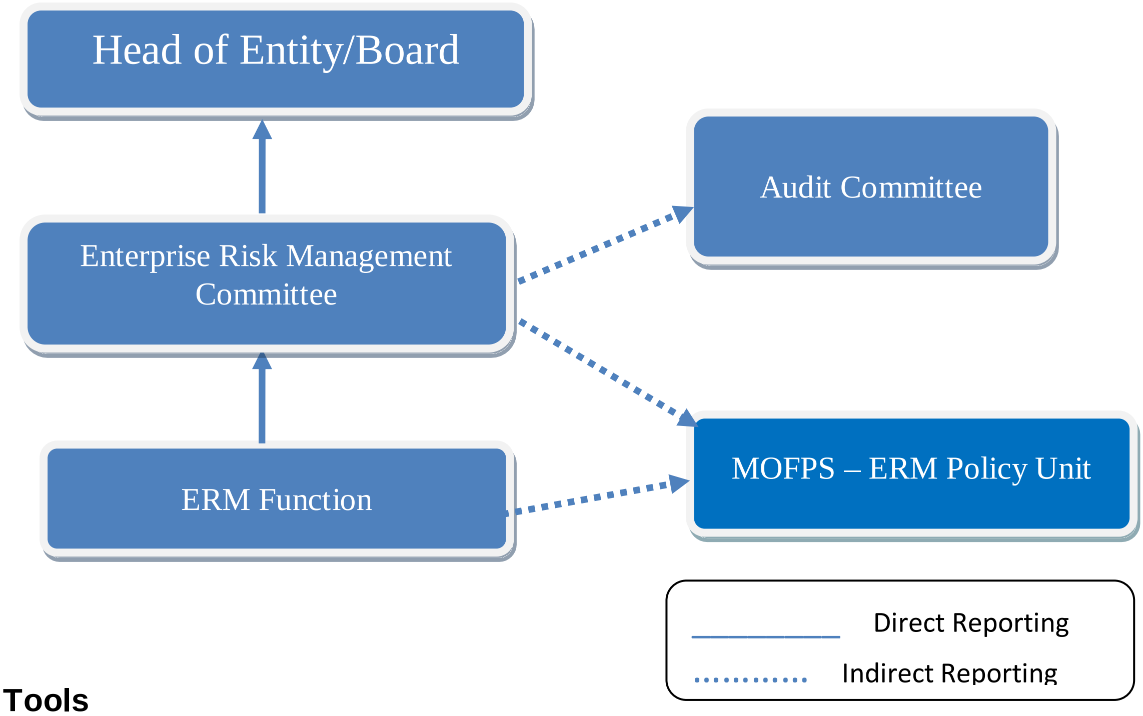
Additional areas/questions that must be answered in the Risk Committee Charter/Terms of Reference include the following:

1. Will the chair position rotate, or will he/she be appointed or reappointed by vote or other means?
2. How will the chair, the committee, and its members be evaluated?
3. What will be the reporting relationship to the risk committee where there are risk champions in related agencies?
4. Which risks will the risk committee oversee, and which will be left to the audit committee?
5. How will the Head of Entity/Board ensure that the risk committee/risk champion has access to the people and resources it will need to carry out its responsibilities?
6. In the case of Statutory Bodies, the decision to establish a separate Risk Committee from the Audit Committee is up to the Board. Consideration of the size, complexity and the ability to ascertain the requisite skill set to sit on the committees must be assessed to arrive at a decision.

3.2.2.1.2. The ERM Structure and Tools

The ERM reporting structure for the GOJ in both a small and large MDA, is set out below. It outlines that the function must report through the Risk Committee to the Head of Entity or the Board. There must also be a reporting relationship to the Audit Committee of the entity as well as the Ministry responsible for finance, on the Risk Management of the respective entity.

ERM Structure



ERM Tools

ERM tools are systems and techniques used to make the risk assessment process simpler to analyse and make decision. It is important to define what you need the tool to do and the data you need to analyze, before selection. Ultimately, the tool must support the process. When selecting a risk analysis tool, consider these criteria[4]:

1. **Aligned to risk analysis objectives:** Does the tool support what the organization is trying to accomplish? What is the aim, an ongoing risk management process or conduct a one-time risk analysis?
2. **Supports decision making:** will the tool provide the necessary information to support decision making?
3. **Accessibility:** How accessible is the tool to users and key stakeholders?
4. **Availability of data:** Is data available for the tool to analyze?
5. **Level of detail:** Does the tool give sufficient information to support decision making?
6. **Integration with other program management / systems engineering processes:** Can the tool integrate with other program / systems?

[4] https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools

3.2.3.Risk Strategy

3.2.3.1. Risk Appetite and Tolerance

Setting the risk appetite and the risk tolerance are the first steps in the process of conducting the risk assessment process. Risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept[5].

A risk appetite is a high-level statement that broadly considers the levels of risk that management deems acceptable. It is related to the longer-term strategy of what needs to be achieved and the resources available to achieve it, expressed in quantitative criteria. In other words, it is the total risk that the organization can bear in a given risk profile, usually expressed in aggregate while risk tolerances are narrower and set the acceptable level of variation around objectives[6]. The tolerance level of risk for an organization is **not** set on an aggregate level but per individual risk with a minimum and a maximum point for each.

The risk appetite in relation to the Government of Jamaica, is the amount and type of risk it is willing to accept to meet its objectives or to take advantage of an opportunity. The level of risk appetite depends on the nature and type of activities under consideration. Therefore, a risk appetite is entity focused and will vary according to the objectives of the entity. For example, the risk appetite in terms of treasury management will not be the same as the risk appetite in terms of technological innovation. Risk appetites also vary over time and the GoJ risk appetite must be reviewed and adjusted to reflect the experience of working with it and the expectations at that time.

The GoJ risk appetite is established and communicated each year in the Fiscal Policy. Therefore, respective entities should be guided by the overall risk appetite of the government when crafting their own risk appetite. **Appendix 9** provides examples of the risk appetite that each MDA can use as a guide.

It must also be mentioned that a Risk Statement is useful but may differ from the risk appetite measures depending on how it is stated. The measures have been explained above and it should be noted that there must be a practical way to assess whether the operations are in line with the guardrails set out by way of the risk appetite measures. While the risk

[5] https://reciprocitylabs.com/resources/whats-the-difference-between-risk-appetite-vs-risk-tolerance/

[6] https://enablon.com/blog/risk-appetite-and-risk-tolerance-whats-the-difference/#:~:text=The%20Relationship%20Between%20Risk%20Tolerance,profile%2C%20usually%20expressed%20in%20aggregate.

statement is a brief on the overall acceptable risk level based on the strategic objectives of the entity, it is usually stated in qualitative terms. It must be noted that some entities combine both measures and statement together. The important point is that the risk appetite must be measurable. Research has shown that without a practical means of measurement, the risk appetite has been proven to be useless. - Carol Williams (2019), "7 Questions for understanding the fundamentals of risk appetite".

The risk appetite should focus on what the organization needs to do to achieve its goals and not so much on the acceptable level of the individual management's risk appetite (Matthew Shrinman, (2017)- "How Management Can Enable Growth"). For example, the statement should denote the level of risk it is willing to take to operate in a globally changing world of technology instead of a management perspective of cyber security issues. The risk appetite should include both internal factors such as longer-term objectives of the entity, risk culture, financial stability of the entity, and external factors such as public image and public needs.

To summarize, the risk appetite and the risk tolerance levels should be crafted based on the strategic objectives of the entity. Therefore, to set these levels, a deep understanding of what are the ultimate goals of the entity, and the respective risk needs, must be defined.

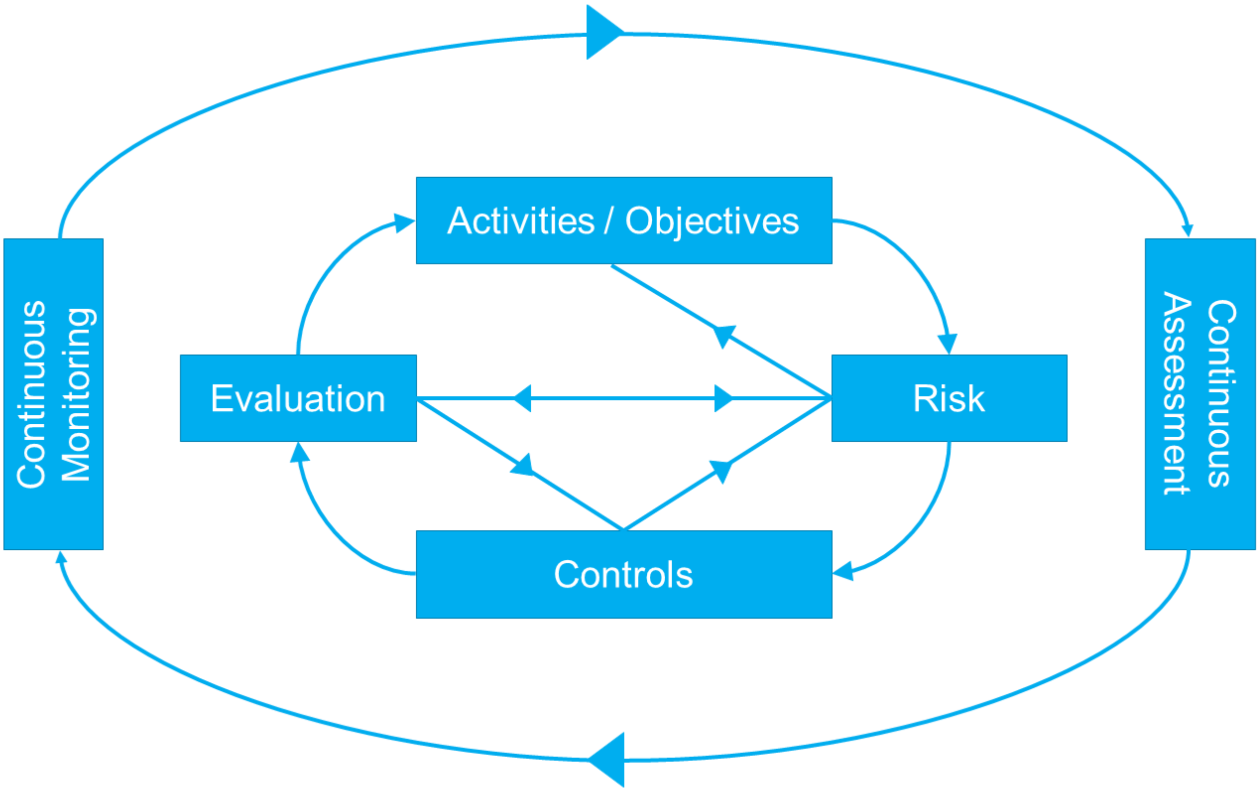
3.2.3.1.1. Risk Assessment Criteria

This is explained in detail in Section 3.3.4 Risk Management Process and **Appendix 5**. The risk assessment criteria set out how the risk will be measured; therefore, it will be entity specific. To establish/determine the criteria to be used, extensive knowledge of the entity is required. The process will also entail setting tolerance levels.

3.2.4. Risk Management Process

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

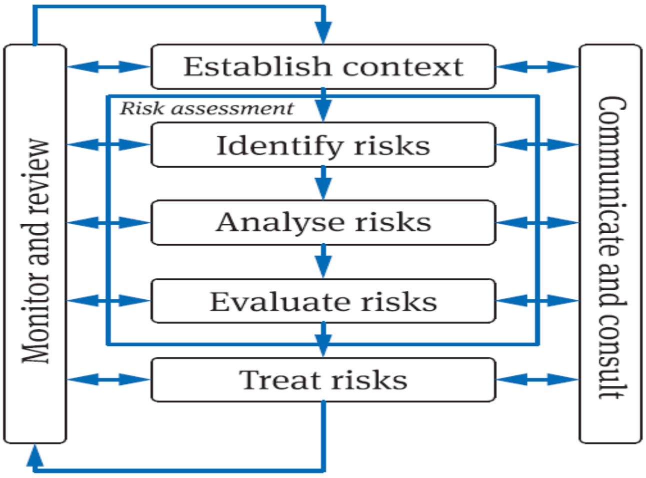


3.2.4.1. The risk management process: practical steps

The risk management process is organised into six main stages:

1. Establishing the context
2. Identifying risks
3. Analysing 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 Process[7]



3.2.4.2. 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.

3.2.4.2.1. 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:

- 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

[7] Adapted from The ISO 31000: 2009 Risk Management Process

will have no obvious timing requirements and so will need to be fitted into the normal work programme.

3.2.4.2.2. 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.

3.2.4.2.3. 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 this 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, 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?

3.2.4.2.4. 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 stakeholders identified in 3.2.1.1 above.

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

- Consult the stakeholders 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'?[8]
- 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;

[8] 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.

- 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 and dealt with in everyday processes.

It is important at this point to spend time focussing 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)?

3.2.4.2.5. Describing risks

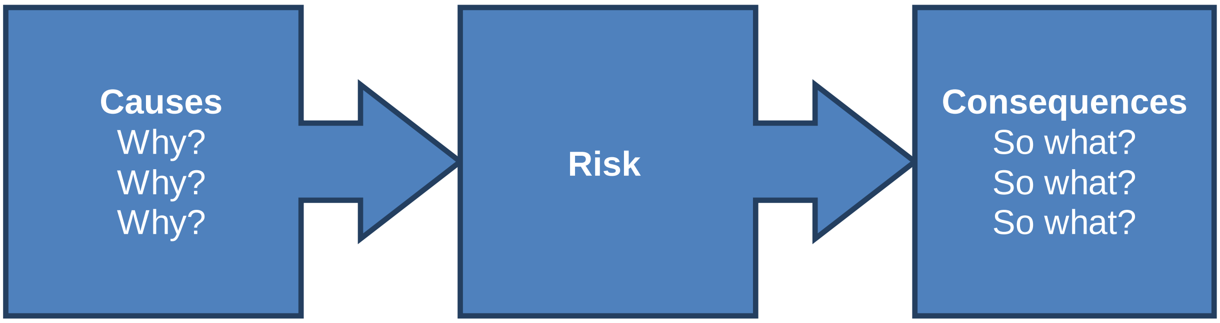
Once identified, a risk must be clearly described. This will enable you both to assess its magnitude and, more importantly, to develop actions that are likely to manage it effectively. A good risk description will:

a) Provide a clear link to the objective(s) that it might affect;

b) Explain both why it is a risk (the causes) and why it matters (the consequences);

c) Look beyond the obvious and explore underlying causes and subsequent consequences;

d) Be more than just a statement of the opposite of the objective



I. Causes

Risks almost always have more than one causes, and the causes may be immediate (the event that finally causes the risk to materialise) 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 2**), or to list them out as bullet points in a logical order (a form for capturing this information is provided in **Appendix 3**).

II. 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.

Again, it is helpful to understand the hierarchy of the consequences that you have identified, using the same approach described in 2.2.1.1. above.

III. Grouping risks

Risks are grouped to identify common themes, risks that are more effectively dealt with together and risks that cross organisational 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 with the details included in **Appendix 4:**

- **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
    - **Human Capital:** risk relating to capability, capacity, connection, cost and compliance
- **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, that is, business continuity risks

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.

3.2.4.3. 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 prioritisation.

3.2.4.4. Assessing risks

There are three levels of appraising risk: inherent, current (or residual) and target. Except in the rare cases where statistical data is 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. Below are details of the 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 prioritise risk activities to manage your more significant risks;
- **Target risk** is where you anticipate what 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 do not yield sufficient value.

Risks are scored on two parameters: likelihood and impact, with risk prioritisation 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 in **Appendix 5**.

Impact is assessed through a judgement of the potential outcome should the risk materialise, 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 in **Appendix 5**.

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 2.5). The risk map is provided in **Appendix 6**.

3.2.4.5. Treating risks

Depending on the level of exposure and risk appetite (see Section 2.5.4. below), you must take a decision on whether to:

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

3.2.4.5.1. 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.

3.2.4.5.2. Managing the risk

There are three basic methods of managing risks:

I. Avoiding the risk

This is achieved either by deciding not to proceed with the activity that creates the risk, choosing an alternate, 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.

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

III. 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. Therefore, as part of the actionable activity each entity should develop a **Business Continuity Plan (BCP) and a Disaster Recovery Plan (this is a**

subset of the BCP) to minimise 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.

IV. Guidelines to develop a Business Continuity Plan

A Business Continuity Plan (BCP) is a mitigation strategy that outlines how a business will operate if there is a disaster, emergency, pandemic, etc. This plan must be documented and include what, who and how business will continue to operate until some semblance of normality is returned. (See template for BCP at **Appendix 10**).

The development of a BCP includes the following steps:

7. Doing a business impact analysis to identify time-sensitive or critical business functions and processes, and the resources that support them. This includes organizing a business continuity team and compiling a business continuity plan to manage a business disruption.
8. Identifying critical Information Technological resources. This will inform your Disaster Recovery Plan.
9. Testing and conducting simulation exercises to evaluate recovery strategies on the plan.
10. Training for the business continuity team.

Once the information has been gathered, it must be mapped to give clear direction on how a disruption will be managed.

Business continuity impact analysis identifies the effects resulting from disruption of business functions and processes. It also uses information to make decisions about recovery priorities and strategies as per the critical operations of the entity.

Resource Required – after an incident has occurred to disrupt the business operations, resources will be needed to carry out recovery strategies and to restore normal operations. Resources can come from within the business or be provided by third parties. Resources include:

11. Employees.
12. Office space, furniture and equipment.
13. Technology (computers, peripherals, communication equipment, software and data).
14. Vital records (electronic and hard copy).
15. Production facilities, machinery and equipment.
16. Inventory including raw materials, finished goods and goods in production.
17. Utilities (power, natural gas, water, sewer, telephone, internet, wireless).
18. Third party services

Information technology (IT) includes many components such as networks, servers, desktop and laptop computers and wireless devices. Therefore, recovery strategies for information technology (Disaster Recovery) should be developed so technology can be restored in time to meet the needs of the business. Manual workarounds should be part of the IT plan so business can continue while computer systems are being restored.

Recovery Strategies - If a facility is damaged, a machine breaks down, a supplier fails to deliver or information technology is disrupted, business will be impacted and the financial losses can begin to grow. Recovery strategies are alternate means to restore business operations to a minimum acceptable level following a business disruption.

Since all resources cannot be replaced immediately following a loss, managers should estimate the resources that will be needed in the hours, days and weeks following an incident to keep the business/operations going.

All these considerations are expected to be captured in a BCP and must become priority in developing a mitigating strategy.

3.2.4.5.3. 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 do 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 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 in **Appendix 7**), which is discussed further in the Risk Policy.

3.2.4.6. Reviewing and reporting

The basic risk management tool is a risk register, which records the risk and its owner[9], its causes and consequences, current and planned controls and risk scores. A risk register template is included in **Appendix 8**. The GoJ maintains a number of risk registers:

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

- **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.

This guidance deals with corporate and operational risk registers, the two that you are most likely to be working with. The principles and techniques are the same for the GoJ risk register and similar for project risk management, but there is detailed guidance on this in the project management methodology[10].

3.2.4.7. Corporate risk registers

The corporate risk register operates at the level of the whole MDA (strategic level) and responds to the need of the Permanent Secretary and senior management to understand and address the risks that might affect delivery of their strategic objectives.

Preparation of the corporate risk register relies on a bottom-up and a top-down approach:

- The bottom-up component relates to risks that have been escalated by others from their operational risk registers and is aimed at ensuring a comprehensive understanding of all key risk exposures. For example, it helps managers to spot a problematic policy or weak operational procedure and escalate it to the appropriate managerial level so that a decision can be taken.
- The top-down aspect aims to distil and provide clarity on the most important risks affecting the MDA's performance, supporting risk-informed decision taking at the top management level and ensuring a risk dialogue at governance level. The top-down process is performed by the Risk Management Working Group, which reviews the overall risk profile of the

MDA, discusses the risks surrounding major decisions and addresses risks raised by the bottom-up process.

The corporate risk register is prepared by the Risk Management Working Group. It is discussed and adopted by the senior management team.

3.2.4.8. Operational risk registers

An operational risk register should be prepared for each major area of activity. This might be by unit, by department, by directorate or by programme. Senior management will determine the most appropriate approach to ensure full coverage of all activities in the most effective fashion. This will determine who is responsible for leading on the preparation of the risk register.

Operational risk registers exist for the use of the associated unit / directorate / department. There are, however, situations where risks should be escalated:

- When the target risk exposure, after all practical actions have been identified, exceeds the risk appetite (i.e., even if all mitigating actions were implemented fully, the risk owner thinks that the exposure to the risk is still too high);
- When the nature of the risk is such that the risk owner has no competence and/or authority in that particular field;
- When the possible mitigating actions go beyond the functional boundaries and so the sphere of influence of the risk owner;
- When a risk is shared with other departments, functions or bodies of the organisation, or it is shared with external organisations, and coordination is needed to find appropriate mitigating actions that can suit all stakeholders

In these cases, the risk must be escalated to the departmental Risk Working Group so that a decision on the risk owner and appropriate actions can be taken. The Risk Working Group may decide to include the risk in the corporate risk register, escalate it for Government consideration or reallocate the risk to another risk owner so that it can be appropriately managed. In the last case, the risk and its mitigating actions will have to be included in the relevant risk register.

3.2.4.9. Reviewing risk registers

Risk registers must be a reflection of the risks that the organisation is currently facing in achieving its objectives. It is vital, therefore, that emphasis is placed on maintaining and updating risk registers rather than simply populating them. Review periods will vary according to the nature of the risks that are on the risk register:

- Corporate risks tend to be long-lasting and slow-moving, and it may be appropriate to review the corporate risk register in detail only a few times a year, perhaps every four months;
- Operational risks tend to be faster-moving, with changes in context (Section 2.1) or actions taken to treat risks (Section 2.5) changing the nature of those risks. Operational risk registers need more frequent review: the appropriate frequency should be determined by the nature of the risks that are faced, but every other month is suggested as a minimum. The review frequency should be stated on the risk register.

A risk register review should cover two questions:

- Are the existing risks still as described or have there been changes?
    - What assurance is there that the current controls are working as expected and are effective in managing this risk?
    - What progress has been made on the planned actions to treat risks?
    - What assurance is there to demonstrate this?
    - Is there any other information that would affect our understanding of this risk?
    - Has the risk score changed?
- Are there any new risks that we should be aware of?
    - Are these risks that could occur now or are these risks that might occur in the future (typically driven by a change that is planned but not implemented yet)?
    - Should something be done now or is this an area that should be kept under review for the time being?

3.2.4.10. Reviewing risk management, including risk performance indicators

The risk management arrangements described in this guidance should be dynamic and respond to changes in the GoJ environment. There must be periodic (at least annual) reviews of the way in which risk management itself is working and the parameters within which risks are managed and judged. These reviews are in addition to any internal audit examinations of risk management, although they may be informed by audit's work. The types of questions to be asked include:

- Are the current arrangements still working?
- Is the risk scoring methodology still relevant?
- How should the risk appetite be adjusted in the light of experience?
- Is there information missing from the risk register and/or is there surplus information in the risk register that could be removed?
- What has been learnt regarding risk management and should changes be made?

4. Risk Management Reporting

The Risk Management Function in each entity must report quarterly on the level of progress of their risk management activity at the Risk Committee meeting and at least once per year to the Ministry responsible for Finance. This report must be based on established indicators.

The Risk Performance Indicators (RPIs) listed below, may be used as part of the overarching review of risk management. Please note, the list is not exhaustive and must be tailored to your entity.

	Indicator	**Target**
1	The number of risk actions not implemented by their due date	
2	Proportion of risks not reviewed at their due date	
3	The number of risks without an owner	
4	The number of controls without an owner	

5	The number of actions without a deadline	
6	The number of actions without an owner	
7	Unidentified risks that have materialised	
8	Identified risks that have materialised	
9	Near misses – unidentified risks	
10	Near misses – identified risks	
11	Risks with a target score at or above the current score	
12	Number of risk register reviews not carried out on time	
13	Number of decisions taken where the risks are assessed to fall outside the risk appetite	
14	Number of reports for decision produced with an incomplete risk assessment	

Appendix 1: Glossary

Term	Definition
Accept	Response to risk taken when the risk is within the organisation's risk appetite. Also known as tolerate or retain
Appetite	The 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 to 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
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 organisation
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?
Control	Actions to reduce the likelihood and/or impact of a risk
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.

Term	Definition
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 (DRP)	Plan for use in the event of a serious loss, such as IT failure, fire or earthquake to assist the 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 level 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 company; 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

Term	Definition
	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 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 materialising
Professional Evaluation and Certification Board (PECB)	PECB is an ISO/IEC 17024 accredited certification body that provides education and certification against internationally recognized standards such as International Organization for Standardization.
Project risk	Project risks are those that could cause doubt about the ability to deliver a project to time, budget and quality
Reduce	Response to a risk that can be (further) reduced by introduction of cost-effective controls. Also known as control or treat 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

Term	Definition
	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.[11]
Risk Appetite	The 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 to 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 a bank will accept, or avoid, in order to achieve its business objectives. It includes quantitative measures expressed relative to earnings, capital, risk measures, liquidity 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 organisation
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.
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.

[11] Institute of Internal Auditors: International Practices Framework

Term	Definition
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.[12]
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 organization to achieve its long term objectives.
Spotting control	A control that will identify that a risk is about 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 risks are very directly linked to the over-arching plans of the organisation

[12] Ibid

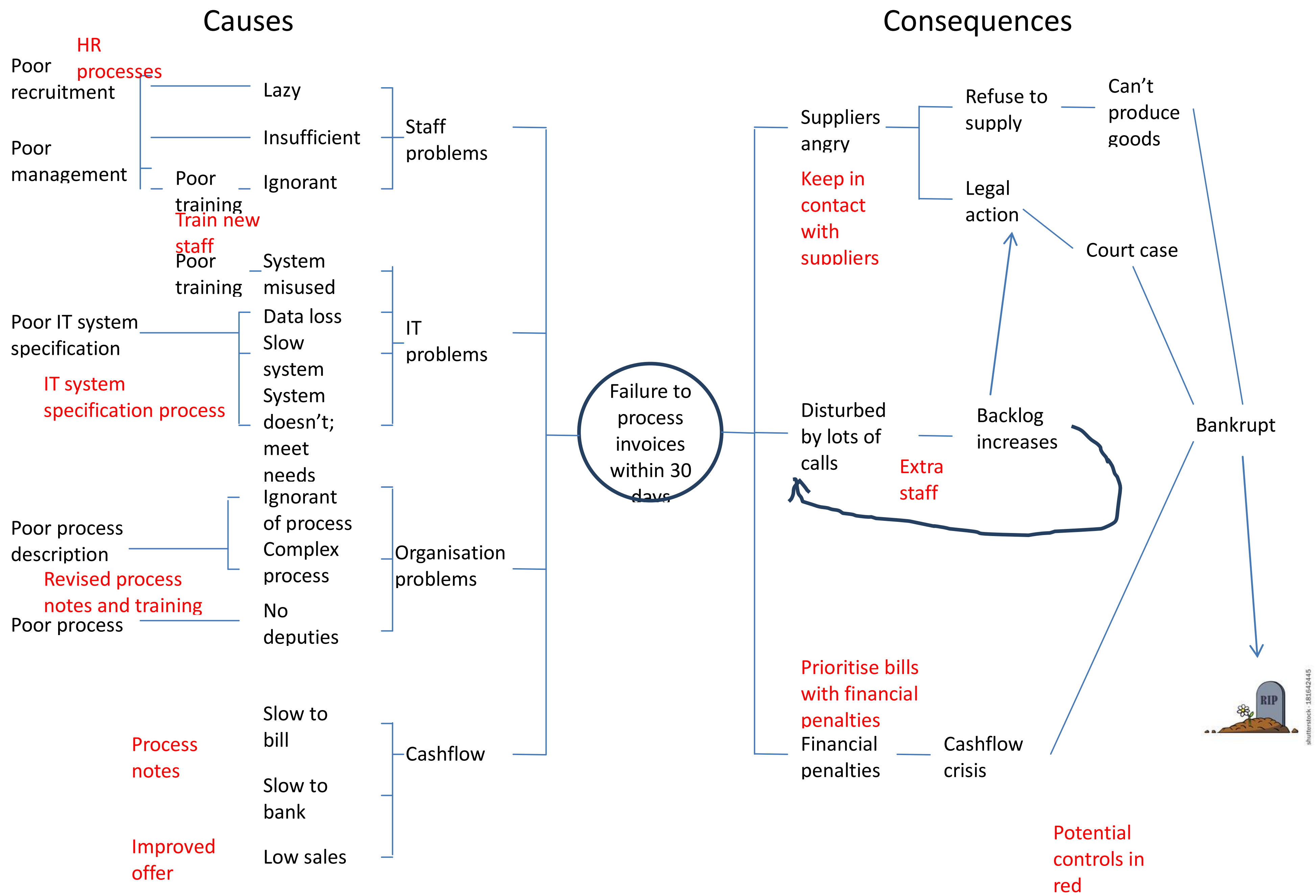
Term	Definition
Target risk score	The level of risk that it is anticipated once all planned actions have been implemented
Transfer	Response to a risk that is outside the organisation's risk appetite that can be shared with or transferred to others, by means of insurance, contract, joint venture, partnership or similar arrangements
Treat	Response to a risk that can be (further) reduced by introduction of cost-effective controls. Also known as control or reduce or mitigate

Appendix 2: 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

Poor recruitment

HR processes

Poor management

Lazy

Insufficient

Poor training

Ignorant

Train new staff

Staff problems

Poor training

System misused

Poor IT system specification

IT system specification process

Data loss

Slow system

System doesn't; meet needs

IT problems

Poor process description

Revised process notes and training

Poor process

Ignorant of process

Complex process

No deputies

Organisation problems

Process notes

Slow to bill

Slow to bank

Improved offer

Low sales

Cashflow

Failure to process invoices within 30 days

Suppliers angry

Keep in contact with suppliers

Refuse to supply

Can't produce goods

Legal action

Court case

Disturbed by lots of calls

Backlog increases

Extra staff

Bankrupt

Prioritise bills with financial penalties

Financial penalties

Cashflow crisis

Potential controls in red

Appendix 3: Risk identification form

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

Appendix 4: 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

Appendix 5: 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[13] 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
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

[13] Parameters need to be set dependent on each entity to which this is applied

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

Appendix 6: Risk map (inherent risk)

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 inherent risks facing the organisation. The heat map can also be done based on the residual risk, where the controls in place are ascertained and used to reduce the inherent risk.

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 risk level. *Note, the heat map below is weighted towards the inherent risk not the residual risk.*

Impact	**Catastrophic (4)**	(CxHU=4)	(CxU=8)	(MxL=12)	(MxL=16)
	Major (3)	(MxHU=3)	(MxU =6)	(MxL=9)	(MxL=12)
	Moderate (2)	(MxHU=2)	(MxU=4)	(MxL=6)	(MxL=8)
	Minor (1)	MxHU=1)	(MxU=2)	(MxL=3)	(MxA=4)
		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.

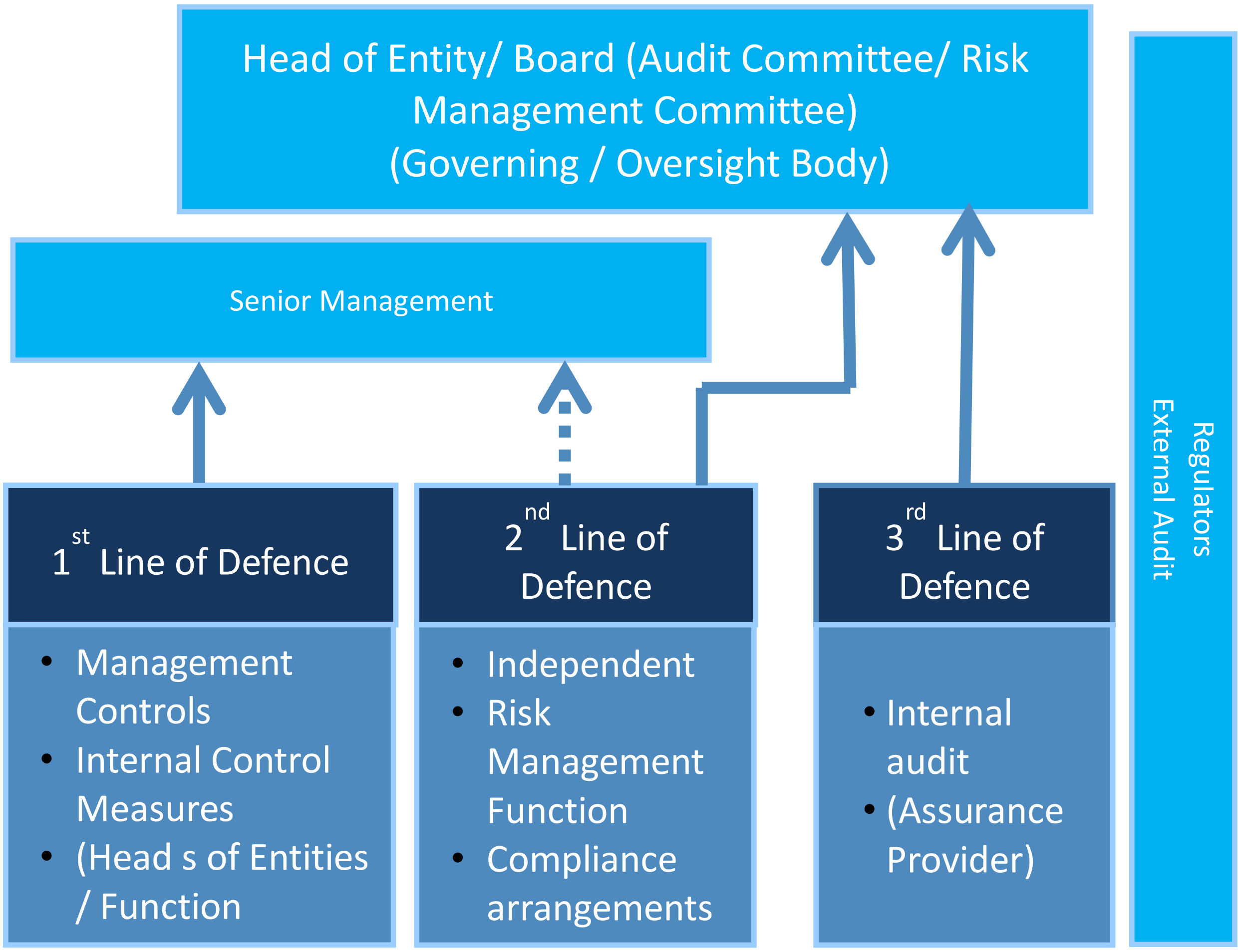
8-11 – Medium – Amber
Medium risk exposure: the risk has the potential to cause harm and could become a high risk. Cost-effective actions should be taken to reduce the level of risk to green and the risk should be routinely monitored for changes that could move it into the red zone.

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 7: Three lines of defence

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 3: 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 includes in internal audit and other internal assurance providers and 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.

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**[14]		**Further actions**	**Who**	**When**	**Assurance on future actions**	**Target risk score**[15]	
							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 ***(Bow Tie method of analysis can be used to ascertain this)***	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 ***(Internal Audit Function can be used to independently assess the control)***			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		

[14] Residual risk score is the score with current controls in place and reflects the efficacy of those controls

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

Appendix 9: Risk appetite description

The risk appetite description must be based on the objective and current situation of the particular government entity

Risk levels and description **Key elements**	**Minimal** **As little risk as reasonably possible**	**Cautious** **Prefer safe delivery options**	**Open** **Consider all potential options**	**Seek** **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 Up to 2% change of exposure	Likely to be minimum controversy Win over doubters easily Litigation over trivial matters only and easily won Up to 5% change of exposure	Some controversy expected Likely to create lingering but low-level dissension Potential for significant litigation that could result in financial loss Up to 7% change of exposure	Plans are controversial Expect continuing dissension Litigation likely and may result in significant loss Up to 10% change of exposure
Innovation, Quality	Innovations avoided unless essential or commonplace Decision making by senior management Essential systems or technology development only Little financial impact each year	Prefer status quo and avoid innovation Decision taking generally by senior management Limited systems or technology development Up to 5% financial and operational impact each year	Innovation supported Non-critical decision making devolved Routine systems or technology development 5-15% financial and operational impact each year	Innovation pursued High levels of devolved authority New technologies seen as key enabler of operational delivery Over 15% financial and operational impact each year.
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

	Little chance of negative exposure to 1 each year	Chance of negative exposure 3 for the year	Chance of negative exposure 4 for the year	Chance of negative exposure greater than 4 for the year
Impact on human resource capacity	Insignificant capacity impairment 0-2% chance of impact	Limited impact on business processes 2-5% chance of impact on resource capacity	Will undermine the Ministry's ability to deliver services on a timely basis 3-10% chance of impact on resource capacity	Could cripple the MDAs that rely on the Ministry for financial resources and policy direction Over 10% chance of impact on resource capacity.
Appetite	**Low**	**Moderate**	**High**	**Significant**

Appendix 10: Business Continuity Plan (Ready Business, n.d.)

Ministry Name:

Address:

Date First Issued:

Revision Date:

Program Administration

Define the scope, objectives, and assumptions of the business continuity plan.

Business Continuity Organization

Define the roles and responsibilities for team members

Identify the lines of authority, succession of management, and delegation of authority.

Address interaction with external organizations including contractors and vendors.

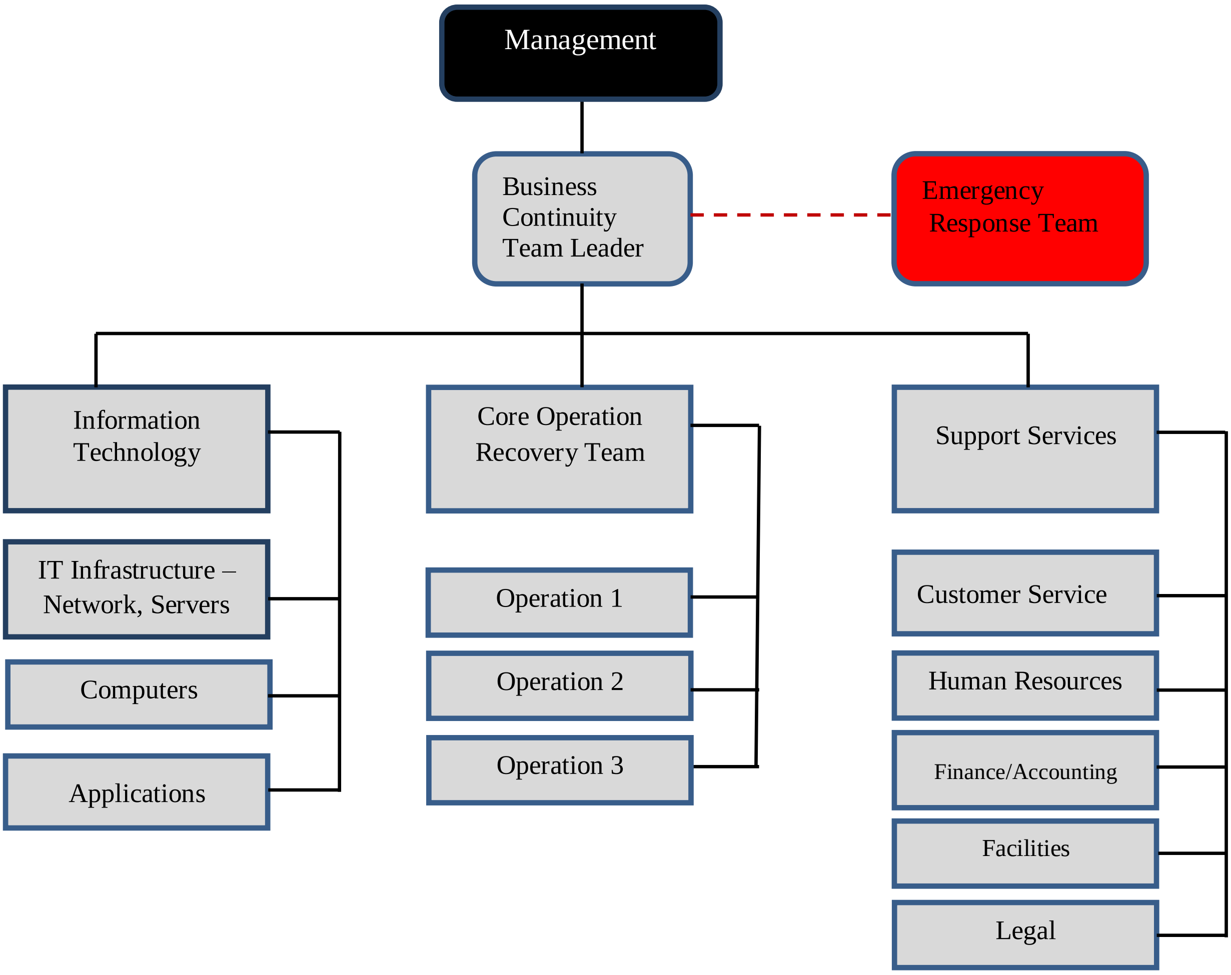


Figure 1. Example Business Continuity Team Organization Chart

Team (IT, Core Operations, Support Service)	Member Name	Email	Work Telephone	Home/Cell Telephone

Business Impact Analysis

- Insert results of Business Impact Analysis
- Identify Recovery Time Objectives for business processes and information technology
- Identify Recovery Point Objective for data restoration

Business Continuity Strategies and Requirements

- Insert detailed procedures, resource requirements, and logistics for execution of all recovery strategies.
- Insert detailed procedures, resource requirements, and logistics for relocation to alternate worksites.
- Insert detailed procedures, resource requirements, and data restoration plan for the recovery of information technology (networks and required connectivity, servers, desktops/laptops, wireless devices applications, and data).

Manual Workarounds

- Document all forms and resource requirements for all manual workarounds.

Incident Management

Define procedures:

- Incident detection and reporting
- Alerting and notifications
- Business continuity plan activation
- Emergency operations center activation
- Damage assessment (coordination with emergency response plan) and situation analysis
- Development and approval of an incident action plan

Training, Testing & Exercising

- Training curriculum for business continuity team members
- Testing schedule, procedures, and forms for business recovery strategies and information technology recovery strategies
- Orientation, tabletop, and full-scale exercises

Program Maintenance and Improvement

- Schedules, triggers, and assignments for the periodic review of the business continuity and IT disaster recovery plan
- Details of corrective action program to address deficiencies.

Appendix

References to Related Policies & Procedures

- Emergency Response Plan
- Information Technology Disaster Recovery Plan (if not included in the business continuity plan)
- Crisis Communications Plan
- Employee Assistance Plan

External Stakeholders:

Ministry/Agencies	Contact Name	Emergency Telephone	Business Telephone
Fire Brigade			
ODEPEM			

Revision History

Revision No.	Date	Description of Changes	Authorization

Plan Distribution & Access

The Plan will be distributed to members of the business continuity team and management. A master copy of the document should be maintained by the business continuity team leader.

Provide print copies of this plan within the room designated as the emergency operations center (EOC). Multiple copies should be stored within the EOC to ensure that team members can quickly review roles, responsibilities, tasks, and reference information when the team is activated.

An electronic copy of this plan should be stored on a secure and accessible website that would allow team members access if company servers are down.

Electronic copies should also be stored on a secured USB flash drive for printing on demand.