Jamaica Deposit Insurance Corporation (JDIC)

Enterprise Risk Management Policy and Framework

Version 1.2 dated September 7, 2023

Table of Contents

ER 1. ERM POLICY

Scope

This Enterprise Risk Management (ERM) policy formalizes the JDIC's risk management program and articulates the roles and responsibilities of the Board of Directors, Board Committees, Management and Staff. This policy provides management with the tools to effectively deal with uncertainty and associated risks and opportunities, thus enhancing the JDIC's capacity to build value by addressing the business risks which could influence the attainment of JDIC's goals and objectives.

JDIC's risk management system is guided by the key requirements of the COSO[1] ERM Integrated Framework and ISO 31000 risk management standard[2].

Definitions

Enterprise Risk Management (ERM) is a process effected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise. It is designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the entity's objectives.

Risk strategy is the way in which JDIC undertakes risk management.

Risk culture is the system of values and behaviors present in an organization that shapes risk decisions of management and employees.

Risk infrastructure is the governance structure that is required to oversee the ERM process across JDIC as well as the operational structure that is required to actually embed ERM in the strategic planning process as well as daily operations. Risk management roles and responsibilities are also clearly defined as well as the technologies that are meant to support the ERM process.

Risk process is the method used in identifying, assessing, managing, reporting and monitoring risks that could positively or negatively influence JDIC's business objectives.

Events – Risks and Opportunities – is the chance of something happening that will have an impact upon objectives. An event can have a negative impact, a positive impact, or both. Events with a negative impact represent risks, which can prevent value creation o**r erode existing value.** Events with a positive impact may offset negative impacts or represent opportunities.

Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities. (Committee of Sponsoring Organizations (COSO))[3]

Three Lines of Defense are defined as follows:

i. First Line: The business line leaders – i.e. Executives have "ownership" of risk, whereby it acknowledges and manages the risk that it incurs in conducting its activities. The first line is responsible for identifying, measuring and reporting risk on an enterprise-wide basis.

---

[1] The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

[2] International Organization for Standardization (ISO) 31000 is intended to be a family of standards relating to risk management codified by the International Organization for Standardization.

[3] COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. The private "sponsoring organizations" includes the five major financial professional associations in the United States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Financial Executives Institute (FEI), the Institute of Internal Auditors (IIA), and the Institute of Management Accountants (IMA).

ii. Second Line**:** The risk management function is responsible for coordinating and supporting the first line of defense in executing their risk management responsibilities, independently from the first line of defense. The second line provides "challenge" to the first line through reviewing its risk assessments and risk responses. The compliance function (General Counsel) is also part of the second line of defense.

iii. Third Line: The internal audit function is charged with the third line of defense, conducting risk-based and general audits and reviews to provide assurance to the board that the overall governance framework, is effective and that policies and processes are in place and consistently applied (Basel). The external auditors and the regulators are often times considered to be part of the third line (or some quarters say the "fourth line") as they too are independent of the first and second line and are expected to provide assurance as to the level of compliance of the first two lines of defense over risk and control procedures.

iv. Fourth Line: The external auditors, as they too are independent of the first and second line and are expected to provide assurance as to the level of compliance of the first two lines of defense over risk and control procedures

Risk - is an event or action that can result in a divergence from expected results, positive or negative, thus impacting the attainment of business objectives and the execution of strategies.

Risk Appetite –is the degree of risk, on a broad-based level, that a company or other entity is willing to accept in the pursuit of its goals (COSO). In other words, it is the amount of risk exposure, or potential adverse impact from an event that the JDIC is willing to accept/retain.

Risk Universe – is the totality of all business risks faced by the JDIC.

Risk Register – is a list of risks that need to be actively monitored and managed. The Risk Register analyzes risks and drives action to:

- Reduce the likelihood of the risk occurring.
- Increase the visibility of the risk.
- Increase the ability to handle the risk, should it occur.
- Reduce the impact of the risk, should it occur.

Strategic Risk – is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. The key elements of strategic risk are related to the political, economic, regulatory environment, global market conditions, legal risk, changing customer needs, and the JDIC's strategic performance measures.

Reputational Risk -is the current or prospective risk to earnings and capital arising from adverse perception of the image of the JDIC on the part of customers, counterparties, or regulators.

Operational Risk – is the risk arising from execution of the JDIC's business functions and focuses on the risks arising from the people, technology, systems and processes through which the JDIC operates. This includes reporting systems, human and resources management systems.

Compliance Risk – is the risk of legal or regulatory sanctions, financial loss, or loss the JDIC may suffer to its reputation as a result of its failure to comply with all applicable laws, regulations, and codes of conduct and standards of good practice (together, laws, rules and standards").

Financial Risk – is the risk of a possible future change in one or more of the following variables: a specified interest rate, financial instrument price, foreign exchange rate, index or prices or rates, or other variable. The most prominent type of financial risk is Market Risk; which is the risk to an institution

resulting from movements in market prices, in particular, changes in interest rates, foreign exchange rates, credit spreads and equity. Liquidity Risk also falls under financial risk and is the probability of loss arising from a situation where (1) there will not be enough cash and/or cash equivalents to meet JDIC's needs, (2) sale of illiquid assets will yield less than their fair value, or (3) illiquid assets will not be sold at the desired time due to lack of buyers.

General Policies

The JDIC recognizes that an overall, unified enterprise risk management programme is required to ensure that all risks facing the JDIC are identified and appropriately managed.

ERM will provide the JDIC with a systematic way to deal with business uncertainty and the associated risks and opportunities. By utilizing disciplined risk and compliance management programs, the JDIC will manage its unexpected outcomes and reduce the impact of risks events when they occur.

The JDIC believes that its business risks can be best managed using an integrated and holistic approach, within an Enterprise Risk Management (ERM) programme. Such a programme will be owned and coordinated by the Executive Management Team, aligned to the strategic objectives of the JDIC, integrated into the managerial and formal reporting process and embedded within the JDIC's culture.

ER 1.01 (a) Achievement of Objectives

Within the context of the JDIC's established mission and vision, Management must establish strategic objectives, select strategy, and set aligned operational objectives cascading through the JDIC.

This Enterprise Risk Management framework is geared to achieving the JDIC's objectives, set forth in four categories:

1. Strategic – high-level goals, aligned with and supporting its mission

2. Operations – effective and efficient use of its resources

3. Reporting – reliability of reporting

4. Compliance – compliance with applicable laws, regulations policies and procedures.

ER 1.01 (b) Components of the JDIC's Enterprise Risk Management Framework

This section provides an overview of the four key building blocks of the ERM framework which are meant to be used to accomplish the objectives of the risk policy.

(i) Risk Strategy

A well-defined strategy for managing risk is essential for appropriate resource allocation (what is being managed and how).

The JDIC's risk strategy is reflected in its risk appetite, risk tolerance and the factors that are considered in determining how risks are prioritized and managed.

(ii) Risk Culture

Risk culture seeks to address:-

a. Where risk ownership starts and stops,
b. The need for risk management training at the appropriate levels
c. Developing proper systems that will promote the right kind of attitudes and behaviors towards risk management

d. What the JDIC must do to achieve its mission.

(iii) Risk Infrastructure

Risk infrastructure covers the risk governance structure that is required to oversee the ERM process across the JDIC and the operational structure that is required to actually embed ERM in the strategic planning process as well as daily operations.
Risk management roles and responsibilities are also clearly defined in addition the technologies that are meant to support the ERM process.

(iv) Risk Process

The Risk process for JDIC will nurture its risk register and will classify the risks into the six risk categories to which it is predominantly exposed. The Risk Process will be supported by appropriate technology.

ER 1.01 (c) Risk Universe

The JDIC's Risk Universe encompasses all business risks faced by the JDIC (i.e. risks affecting all of the JDIC's objectives) and these include the following:

1. Strategic Risk
2. Reputational Risk
3. Operational Risk
4. Compliance Risk
5. Financial Risk

ER 1.01 (d) Risk Appetite Statement

Risk appetite statement establishes JDIC's risk appetite for the 5 risk categories (see ER 1.01c above) to which it is exposed. See section "ER 2, Risk Appetite" below for further details.

Communication of ERM

Primary responsibility for identifying and assessing the risks, regardless of category rests with the first line of defense (i.e. Executive Management).

The Risk Manager will provide supporting tools and time to check and challenge the first line of defense and is generally responsible for consolidating and issuing risk reports to the respective board level committees.

The first line of defense (Executives) must update their risk registers and submit them to the Risk Manager for independent review and analysis on a periodic basis (at least quarterly). Risk management updates must be an agenda item at Management meetings.

ER 2. ERM Framework: Risk Strategy

Risk Appetite

Risk appetite speaks to the amount of risks that JDIC is prepared to take while pursuing its strategic and operational goals. JDIC's overarching risk appetite statement is as follows:

> ***"JDIC has a low risk appetite for strategic, reputational, financial (market, liquidity, credit) and compliance risks and a low to moderate appetite for operational risks".***

As a general rule, JDIC's risk appetite requires the implementation of action plans that seek to reduce residual risks[4] that have been rated as Very High and High to a target rating of at least Moderate or Low depending on the risk in question. The target risk ratings are guided by JDIC's risk appetite statement (see paragraph immediately above).

Risk Tolerance

Risk tolerance is effectively the same as risk appetite, but taken from the opposite perspective. For example, if JDIC has a Very High Risk relating to a Compliance risk (e.g. The corporation may not adhere to regulatory and compliance requirements.), then according to JDIC's risk appetite, this exposure must be reduced to Low, given that JDIC has low risk tolerance for Compliance risk. The foregoing could be expressed in the language of risk tolerance by saying "JDIC will only tolerate risks relating to compliance that are rated as Low."

Risk Assessment Criteria

Risk assessment criteria refers to the standard that JDIC will use to determine how a risk event gets rated.

JDIC has decided that two variables (with the possibility of others being added in the future) will be used to determine how risks are rated – these variables are "impact" and "likelihood". Events that would have the most devastating impact and which are most likely to occur would receive the highest risk ratings, with the highest possible rating for a risk being Very High. The other ratings in order of priority are High, Moderate and Low.

See the Risk Map, in Table 1 below which illustrates this concept further. See also Appendix II for further details on the factors that JDIC takes into consideration in determining impact severity and the likelihood of a risk occurring.

Risk Map

This risk map is a convenient way of summarizing the risk ratings that result from the combination[5] of likelihood and impact for a particular risk event.

---

[4] Residual risk refers to the amount of risk exposure left after considering existing control measures, staff experience, the number of previous occurrences of the risks, and similar factors. The combinations of the Likelihood and Impact of a risk occurring

[5] The combination of the Likelihood and Impact of a risk occuring

Table 1: Risk Map

LIKELIHOOD	IMPACT					
		INSIGNIFICANT	LOW	MODERATE	HIGH	SIGNIFICANT
	VERY LIKELY	Low Risk	Moderate Risk	High Risk	Very High Risk	Very High Risk
	HIGHLY LIKELY	Low Risk	Moderate Risk	High Risk	Very High Risk	Very High Risk
	LIKELY	Low Risk	Moderate Risk	Moderate Risk	High Risk	High Risk
	UNLIKELY	Low Risk	Low Risk	Moderate Risk	Low Risk	Low Risk
	VERY UNLIKELY	Low Risk	Low Risk	Low Risk	Low Risk	Low Risk

Risk Responses

Risk responses (action plans) are required to reduce risk exposures that are outside of JDIC's risk appetite. See Appendix III for a summary of the Risk Responses required to achieve JDIC's risk appetite.

Risk Responses: Timeliness

The higher the rating of a risk, the quicker JDIC desires the risk to be actioned. It is acknowledged that to properly respond to a risk could take one week (or less) or one year (or more).

Accordingly, the timelines required below, are more from the perspective of the risk being assigned an owner who takes responsibility and that there is ongoing reporting on the status of the risk until it has been addressed in a reasonable period of time.

VH: **Very High Risk**; **immediate action is** required by management and a detailed status of the proposed risk response and the related corrective actions are to be reported at each sitting of the relevant management and Board level risk Committees.

H: **High Risk**; action is required by **management** within **three months** or such earlier period as may be necessary in the context of the risk, and a detailed status of the proposed risk treatments is to be reported at each sitting of the relevant management and Board level risk Committees.

M: **Moderate Risk**; The risk response and the related corrective actions should be implemented within **6 to 12 months by management.** A detailed status of the proposed risk response is to be reported at each sitting of the relevant management committee at quarterly intervals at the Board level risk Committees.

L: **Low risk**; No action required. The risk should be monitored on an ongoing basis by management.

Risk Responses: Corrective Actions

Generally, JDIC expects risk exposures beyond its risk appetite to be addressed using one or more corrective actions that seek to either mitigate, prevent, avoid, transfer or accept the risk.

As discussed below there are times when the risks will be recommended for acceptance as this may be deemed the best risk response – see the discussion immediately below over the process required for risk acceptance. See also section 4, Risk Process for more details on the process involved in correcting or mitigating risk exposures.

Risk Responses: Risk Acceptance

There are times when a Risk Owner may recommend that the best risk response for a risk that has been rated Very High or High is to accept the risk. A risk owner on his or her own does not have the authority to accept a risk exposure.

A formal recommendation to accept the risk should be made to the respective management level risk Committee after which it would be referred to the CEO for his or her input and then the relevant Board level Committee that oversees that risk for approval – The relevant Board level Committee would then take the risks to the Board for ratification. The recommendation should be accompanied by a cost / benefit analysis that contemplates the following:

- A description of the risk exposure and the risk rating
- The financial cost of addressing the risks
- The financial and non- financial benefits of addressing the risk
- A conclusion as to whether the costs outweigh the benefits
- An indication as to the period of time over which the risks should be accepted or whether the risk should be accepted permanently
- Regardless of whether the acceptance period for the risk exposure is permanent or temporary – the Risk Owner is required to state any monitoring control activities that can be employed over the course of time that the risk will be accepted.

The formal recommendation to accept the risk should form a part of the Audit Committee's Report to the Board of Directors.

ER 3. ERM Framework: Risk Infrastructure

This section of the framework covers the governance structure that is required to oversee the ERM process across JDIC as well as the operational structure that is required to actually embed ERM in the strategic planning process as well as daily operations.

This section also ensures that the risk management roles and responsibilities are also clearly defined as well as the technologies that are meant to support the ERM process.

Governance and Operational Structure

ER 3.01 (a) Governance Structure

The governance portion of the infrastructure (see Appendix IV) deals with how the oversight role over the risk management process would be executed. The Audit Committee (AC) would be the primary risk oversight Committee, overseeing the activities of the Enterprise Risk Management Committee (ERMC). Other Board Committees would oversee such as Investment and Corporate Governance would oversee risks (e.g. credit) that fall immediately under their oversight

ER 3.01 (b) Operational Structure

The operational structure portion which is graphically depicted in Appendix IV deals with who will be responsible for the daily execution of the ERM process at JDIC.

ERM Roles & Responsibilities

This section describes the specific roles of the key stakeholders in the ERM process.

ER 3.01 (c) Audit Committee

1. Approval of the ERM policy and framework after recommendation for approval by the Enterprise Risk Management Committee;

2. Approval of JDIC's risk appetites[6] after recommendation by the Risk Manager and the ERMC;

ER 3.01 (d) Other Board Level Committees

1. JDIC has other Board level Committees that oversee specific risks affecting the JDIC. These Committees include:

    - Investment
    - Corporate Governance

2. These Committees will meet in accordance with their Charters to discuss and ensure that the specific policies and procedures affecting the risk areas that they oversee are up to date and that the risks are being managed within the stated risk appetites.

3. JDIC's Board will receive the top risk issues affecting these areas periodically along with the status and budgets associated with any mitigating actions.

4. Considers risks i.e. ensures that a strategic risk assessment of the key strategic objectives and the

[6] See definition of Risk Appetite for further details.

related strategic initiatives are done when evaluating the strategic direction of JDIC.

5. Recommends budgets that are required to implement risk responses (corrective actions) that are meant to reduce risk exposures. Works closely with the Chair of the ERMC in understanding the status of risk responses and the key recommendations to be made to the Audit Committee and other Board level committees to mitigate risks. The foregoing includes obtaining detailed risk information on the top risks affecting JDIC's business objectives.

ER 3.01 (f) Enterprise Risk Management Committee

The risk management responsibilities of the ERMC shall include, but not be limited to:

1. The ERMC is constituted of the Executives from across JDIC;

2. Provides an update on the status of the top 10 or 20 risks (strategic and operational risks) at least monthly or other appropriate period and the status of risk responses to the Chief Executive Officer and the Audit Committee;

3. The Enterprise Risk Management Committee will also function as the overall Enterprise Risk Management Committee that reviews the big picture for all risks across JDIC i.e. strategic, operational, reputational, compliance, financial (market risk) and liquidity risks. The Risk Manager will be responsible for consolidating the key risk information for all risks for presentation and discussion at the ERMC Meetings;

4. Recommending changes to the risk appetite and tolerance levels to the Audit Committee, after receiving input from the Risk Manager and the CEO;

5. Ensuring that JDIC through the Risk Manager (who will coordinate with the department heads) has an up to date Risk Register, that reflects existing and emerging risks;

6. Monitoring the status of actions plans (risk responses) that are meant to address Very High and High risk exposures;

7. Recommend the approval of action plans requiring budgets over a certain dollar amount to the CEO and the Audit Committee; and

8. Ensures that all required resources are in place to support the activities of the ERM process across JDIC, including but not limited to reviewing and recommending the approval of the ERM policy and framework and other similar items to the Audit Committee for approval.

ER 3.01 (g) Risk Manager

High level summary of the roles and responsibilities of the Risk Manager, are as follow:

- Consolidation of risk registers received from the business line managers;
- Review of risk registers, for accuracy and providing "independent challenge" on risk mitigation strategies and any other aspect of the risk registers from any department in JDIC;
- Perform periodic risk reviews i.e. spot checks on mitigating controls over risks that could have significant adverse impact on the JDIC;
- Supporting risk champions/owners in updating their department's risk registers, including the strategic risk assessments that support the strategic plan;
- Maintain the risk software, that supports the ERM process;
- Coordinate risk training for all relevant parties;
- Coordinate the annual risk workshop and risk validation sessions;
- Review of new products for compliance with the JDIC's risk appetite before products "go live";
- Conduct Spot checks on major Third Party Contracts for compliance with contractual

arrangements and also provide support in conducting financial and commercial due diligence of such Third Parties before entering into a third party relationship;
- Prepare risk reports for the Board level committees and the ERMC;
- Review internal audit reports – to confirm the strength of internal controls over high risk areas that could have major adverse impact on the JDIC;
- Manage the development and maintenance of a loss events and "near misses" database; and
- Prepares a consolidated report on the overall status of the top risks across all 6 risk categories in the Risk Universe for discussion at the ERMC.

The detailed roles and responsibilities include:

1. The Risk Manager has executive level responsibility for the ERM process at JDIC and will report to the CEO on matters relating to the ERM process, but with a "dotted line" to the Audit Committee when certain circumstances are triggered. These triggers include, and are not necessarily limited to the following:

    - Situations where the Risk Manager, shares a different view from both the CEO and the rest of the ERMC on the risk responses to be pursued on High and Very High risks affecting JDIC;
    - Situations where the Risk Manager, shares a different view from both the CEO and the rest of the ERMC on S rating that is assigned to a risk, where the Risk Manager believes the assigned rating should be High or Very High;
    - At all times, the Risk Manager must advise the CEO of any instance in which he or she intends to take a matter to the Audit Committee under this "trigger clause".

2. The Risk Manager will be the chief facilitator with the risk owners and JDIC as a whole in ensuring that ERM gets embedded across JDIC in accordance with JDIC's Risk Policy and Framework. Specifically, the Risk Manager will:

    - Ensure that the tools, templates or their equivalent that are required to support the ERM process are available and properly configured;
    - The Risk Manager will, with support from others where necessary:
        a. Coordinate and ensure that ERM training is conducted for risk owners, risk champions and other key stakeholders;
        b. Ensure that JDIC's risk assessment criteria[7] are configured in the risk assessment tool or its equivalent. Also, ensures that JDIC's risk appetite and risk tolerances are configured in the ERM risk assessment tool or its equivalent;
        c. Coordinate and facilitate risk assessment workshops at least annually;
        d. Coordinate and review risk registers to ensure that risk responses for significant strategic and other risks are updated by the risk owners to a level that falls within JDIC's risk appetite;
        e. Coordinate to ensure that risk responses are followed up and budgets are allocated where necessary. This is a critical aspect of the work and also extends to checking and reporting that the underlying documentation of the internal controls to mitigate risks are up to date and efficient from a time and cost perspective;
        f. Ensure that periodic Risk Reviews (not audits) are coordinated by the Risk Manager to check if risk responses (internal controls / procedures) continue to be in place to mitigate high impact (scores of 4 or 5). This is another critical aspect of the responsibility of the Risk Manager. Checks can be done every 6 months or any other frequency desired by the ERMC and the Audit Committee;

[7] This is the objective basis on which JDIC will determine how a risk gets flagged as significant or insignificant.

g. Provide direct support (e.g. via risk workshops or interviews) to the first line and their teams in helping to update their risk registers.

3. Ensures that the ERM policy and framework are updated based on ongoing changes to the ERM process;

4. Ensure that tools, templates and the ERM software are highly usable for all stakeholders who participate in the ERM process;

5. The Risk Manager reports shall be submitted to the ERMC for discussion and debate. The CEO and the Risk Manager discuss risk reports before they are submitted to the ERMC. The reports should include but not limited to the following:

    - Quarterly Risk Report which includes the consolidation of the implementation status of risk response / corrective actions for significant risks (Very High and High) across the JDIC;
    - Summary of "near misses" and actual loss events that occurred each month across the JDIC;
    - Root cause analyses / contributing factors of actual losses experienced;[8]
    - Risks that are being recommended for formal risk acceptance to the ERMC where the "cost" of treating or responding to a risk outweighs the benefits;
    - Summary of new risks facing JDIC, which emerged since the last report that was submitted by the Risk Manager as well as an assessment of these risks, related exposures and recommendations for treatments and the associated costs
    - Key risk related trends noted from the internal audit reports submitted by the Internal Auditor
    - Updates on emerging risks in the external environment
    - Test of Controls Report
    - Updated ERM Policy and Framework and ERMC Charter

    - Manage the development and maintenance of a Near Misses and Loss Events database. Also to investigate root causes of losses and Near Misses

6. Coordinate the risk acceptance process – see section 2;

1. Review of internal audit reports – to confirm the strength of internal controls over high risk areas that could have major adverse impact on the JDIC;
2. Review of new products for compliance with the JDIC's risk appetite before products "go live";
3. Conduct Spot checks on major Third Party Contracts for compliance with contractual arrangements and also provide support in conducting financial and commercial due diligence of such Third Parties before entering into a third party relationship.

ER 3.01 (h) Risk Owners

1. Risk Owners[9] are responsible for ensuring that at least on a periodic basis (at least twice per year),

[8] After ERM becomes fully embedded across JDIC, consideration should be given to formally developing key risk indicators (KRIs) as part of the tracking and monitoring of risks. A KRI is an indicator that indicates whether or not a risk may actually be happening. For example, JDIC may have a risk "staff may leave JDIC before JDIC starts to recover its investment in staff costs and training" – a KRI for this risk is the actual staff turnover rate of JDIC.

[9] A Risk Owner is the person that will be held ultimately responsible if a risk was to materialize and there was a loss to the JDIC. Risk Owners

new and existing risks under their jurisdictions are updated in the risk register, all risks are assessed, risk responses are developed and risk responses are monitored until the risk exposure falls within JDIC's risk appetite. Risk owners also have responsibility for logging loss events and near misses in the tool provided by the ERMC;

2. Select risk champions (see section below) who will assist in carrying out all relevant risk management duties that fall on the risk owner.

3. It is the responsibility of the Risk Owners to ensure that, all risks are responded to or treated whether or not the Risk Owners have the technical ability to carry out the risk treatment.

4. Should be required to give a formal explanation (and could possibly be subject to sanctions) if an independent review of the internal controls (Likelihood ratings) over a risk are fundamentally different from the rating in the risk register.

ER 3.01 (i) Risk Champion

The role and responsibility of the risk champions:

1. Risk Champions are nominated by the Risk Owners to assist the Risk Owners in executing their risk management duties, in accordance with the requirements of the ERM Risk Policy & Framework. Depending on the size of a department, it is likely that one person may be the Risk Champion for more than one department.

2. Risk Champions will therefore be required to have access to the Risk Assessment Tool or its equivalent and the Risk Policy and Framework

3. While the Risk Champions are expected to assist the Risk Owners, ultimate responsibility for ensuring that risks are managed in accordance with the Risk Policy & Framework, rests with the Risk Owners

ER 3.01 (j) Internal Audit

The Internal Audit function is a key part of the monitoring function of the risk management governance structure. Internal Audit will independently test the internal controls over the Moderate and Low residual risk areas across JDIC, with an impact score of 4 or 5 to assist in ensuring that the mitigating controls are in fact effective. Accordingly, the Audit Plan of the Internal Audit unit should be guided by risk registers of JDIC.

Internal Audit is required to develop their risk based audit plan, using the results of the risk assessment [10]that is based on the requirements of the JDIC risk policy and framework. Additional responsibilities of the Internal Audit function include:

- Internal Audit is required to perform periodic independent checks to ensure that the ERM process is working as intended and make recommendations for improvements;

- The Internal Audit function is required to supply all final internal audit reports to the Risk Manager, so that the Risk Manager is able to analyze risks trends and the effectiveness of internal controls over key risk areas;

- Internal Audit may be consulted by the Risk Owners and the Risk Manager in discussions

are ultimately the JDIC's Management Team (i.e. heads of departments). They are responsible for ensuring that all key risks in their areas of responsibility are properly managed (mitigated, prevented, avoided transferred or accepted).

[10] Internal Audit reserves the right to examine the process that led to the generation of the risk assessment, and to ask appropriate questions as they see fit, before they use the results of the risk assessment to drive its audit plan. Internal audit may also elect to use other risk assessment techniques alongside the one that is embedded in the ERM process. It is however expected that the Internal Audit unit will find the process used by JDIC to be acceptable

surrounding the development of risk response plans/controls that are expected to mitigate, transfer, accept, avoid or transfer major risks;

- Internal audit is required to seek the input of the Risk Owner before a risk is rated in an internal audit report, especially if the rating will be different from that which was in the risk register (if the risk was previously identified and assessed). Final ratings on internal audit points are owned by the Audit Committee i.e. where there is a difference in opinion as to the risk rating by internal audit and the Risk Owner, the Audit Committee has the responsibility to assign a final risk rating. The risk rating system used by internal audit should be based on the rating that is included in this ERM Risk Policy and Framework – this will ensure one common language and promote consistency across JDIC.

ERM Technologies

JDIC recognizes the importance of using appropriate technologies to support the ERM process. Consequently, JDIC has determined that where feasible appropriate ERM technology should be used to support the following aspects of the ERM process:

1. Risk identification
2. Risk assessment
3. Risk management
4. Risk reporting

ER 4. ERM FRAMEWORK: RISK PROCESS

This section covers the steps that constitute JDIC's ERM risk process; the risk process includes risk identification, assessment, risk response, reporting and monitoring.

Risk Identification

Risks i.e. barriers to achieving objectives, are identified at the strategic level (focusing on the strategic objectives and the strategic initiatives to achieve those strategic objectives) as well as the operational level which cover the business processes in the departments at JDIC. Together these risks encompass JDIC's Risk Universe. Each risk (barrier) is further classified under one of several types of risk categories as follow:

1. Strategic
2. Reputational
3. Operational
4. Compliance
5. Financial

All risks must be identified within the context of a particular business objective i.e. whether strategic or operational.

Strategic Planning Level

i. Each year

When JDIC's strategic objectives and the related strategic initiatives to achieve the objectives (as articulated in JDIC's strategic plan) change, the Risk Manager will coordinate the identification of risks that affect the strategic objectives by providing support to the Executives who own the execution of the various strategic objectives.

ii. Ad Hoc

For new risks identified based on ongoing changes in the environment (or based on the usual updates to the strategic planning process), the strategic risk owners will update their registers accordingly.

ER 4.01 (b) Operational level[11]

i. *Periodically (at least quarterly)*

- Risk Owners are required to formally update the risks affecting business processes in their Risk Registers periodically (quarterly).
- The Risk Owners should formally report addition and removal of risks to the ERMC in the periodic reports submitted by the Risk Manager.

ii. Ad Hoc

[11] This means business processes performed in the functional areas of JDIC

For new risks identified based on ongoing changes affecting business processes in the departments or environment, these should be updated as they occur by the departments. See steps above for the treatment of new risks and the removal of existing risks.

ER 4.01 (c) Risk Taxonomy

Risk taxonomy addresses the basic profile of each risk that falls within JDIC's Risk Register. The risk taxonomy to be used by JDIC (this is not an exhaustive list) as captured in its Risk Register is as follow:

- Objective (whether it is a strategic objective or an operational objective (i.e. business process objective)
- Risk description
- Risk Category: Each risk will fall into one of 5 categories (see section 1 for further details)
- Financial (dollar value) impact of the risk
- Impact Type – This deals with the severity of the impact on JDIC if a risk were to materialize.
- Likelihood – Deals with how likely it is for a risk to materialize based on existing controls and history
- Root Cause or Contributing Factor of a Risk Occurring
- Risk Owner
- Current Residual Risk
- Target Residual Risk
- Planned Risk Response
- Budget needed to mitigate or respond to the risk
- Risk Trend
- Net Value Protected or Enhanced by mitigating the risk (i.e. comparison of the cost to mitigate the risk to impact if the risk were to materialized

Assess Risk

After the risks have been identified at the strategic and operational levels, the risks will then be assessed to prioritise (i.e. given a rating of Very High, High, Moderate or Low) their importance.

JDIC will assess the risks by the **likelihood** of the risks occurring in the next 18 months and the **impact** of the risks if they should occur in this timeframe. As stated in another section, Impact is influenced by both financial and non-financial considerations – See Appendix II for further details.

i. Annually

Risk Manager will coordinate an annual risk validation session for all risks in the Risk Universe.

ii. Periodically (every 6 months)

Risk Owners should re-assess their risks at least every 6 months and share the findings with the Risk Manager for subsequent discussion with the ERMC.

iii. Major projects

- This ERM Framework requires that detailed risk assessments be completed for all major projects (e.g. new IT systems) and that these risks be monitored and appropriate interventions be employed on an ongoing basis. The project sponsor and the Risk Owner

in charge of the department that the project falls under is responsible for ensuring that the detailed risk assessments are done. The relevant project management personnel within the JDIC should also provide project management support to assist in guiding the monitoring and successful implementation of the project.

- The risk assessment approach should be at minimum, based on the risk assessment approach required by this ERM framework.
- This Framework also requires that the Risk Manager and Internal Audit unit, be involved at all stages in all major projects across the JDIC in order to assist in ensuring that key controls are in place to mitigate key risk factors.

Risk Response

Once JDIC establishes the ranking of the risks it faces from the risk assessment process and, by extension, the risk exposures that it finds unacceptable, these risks should then be responded to or be managed within JDIC's risk appetite by the Risk Owners.

The basic objective of the risk management process is to reduce the risk exposures to an acceptable level; generally this is rating of Low or Moderate. This will therefore require budgets to be allocated.

ER 4.01 (d) Risk Appetite

As stated in section 2 (Risk Strategy), risk appetite is set on a principles basis and is applicable to all areas of JDIC. The basic principle is that JDIC will not accept risks that are rated Very High or High (and in some cases Moderate risks will not be tolerated) as determined by the Risk Assessment process.

ER 4.01 (e) Risk Response

i. Based on JDIC's established Risk Appetite, all unacceptable risks (i.e. rated Very High or High) require a Risk Response to be raised to reduce the risk exposure to at least a Moderate or Low rating. Risk Owners have the primary responsibility for determining the appropriate Risk Responses but they can delegate the implementation of the risk response to a Risk Champion. Risk Responses should consider relevant costs and benefits.

The ERMC or other relevant management level risk committee will review the cost of responding to risks and make recommendations to the CEO for approval

ii. Risk Owners will report at least quarterly on the status of their Risk Responses to the ERMC and the relevant Board level committee. The Risk Manager will provide support in the risk reporting process.

iii. Risk responses should be closed, once the required actions have been taken and the Risk Register updated accordingly. Any attendant procedures documents should be updated by the Risk Owner based on the risk response.

Risk Reporting

The CEO, each Board Committee (e.g. Audit Committee) and the related management level risk committee (e.g. Enterprise Risk Management Committee) will receive reports from the respective Risk Owner for the particular risk that is being managed by that risk owner. For example, the Investment Committee will receive risk information relating to financial and liquidity risk from the Director, Finance and Investments.

The Risk Manager will perform a coordinating role in the preparation of the risk reports to the Enterprise Risk Management Committee. In general these reports will fall into the following categories:

- Quarterly / Monthly – Risk Response (Action Plan) Status and Required Budget for High and Very High risks
- Quarterly / Monthly – Top 10 Risks across each risk category Quarterly / Monthly – Risks being recommended for Risk Acceptance
- Quarterly / Monthly – Risk Trends (upwards or downwards) for Top 10 Risks
- Quarterly / Monthly – Risk Ratings that Changed After an Internal Audit or Other Testing

Monitor Risk

ER 4.01 (f) External Scan

i. Sources such as those published by governments, or entities similar to the JDIC should be used in scanning of the external environment. The Risk Manager, will play a coordinating role in assisting in risk owners in quickly identifying, assessing and reviewing such information.

ii. All Risk Owners (first line of defense) will be responsible for scanning the external environment (political, social, environmental, economic and other variables) with a view of identifying new and emerging risks that JDIC faces on a quarterly basis. The scan should be especially within the context of emerging risks that could adversely affect objectives assigned to each Risk Owner.

iii. New and emerging risks identified should then be added to the relevant risk register of the risk owner, after following the process for adding new risks.

ER 4.01 (g) Internal Scan

i. The Risk Manager is required on a quarterly basis to analyze the root causes and contexts / contributing factors of the Very High and High risks in the Risk Universe / risk registers.

ii. This analysis should make reference to the Risk Assessments done by Risk Owners, as well as internal control weaknesses identified in the Internal Audit Reports and any other reports produced for across JDIC.

A report on the scan shall be prepared by the Risk Manager and discussed with the ERMC and the respective risk owners at its meetings with a view of identifying new or changing risks trends that should be added to the Risk Register and be appropriately actioned.

ER 4.01 (h) Monitor the status of Risk Responses

i. The Risk Manager is required to report to the ERMC and the Board, the consolidated status received from the Risk Owners of their risk responses (required to mitigate risks) citing overdue actions and analyzing underlying challenges that may have led to due dates for actions being missed

ii. The CEO should consider relevant sanctions that should be taken for long overdue risk response that are not supported by proper explanations

ER 5. ERM FRAMEWORK: RISK CULTURE

Risk environment deals with how risk management is to be embraced and adopted at JDIC given the vision and mission of JDIC. A number of adjustments and initiatives are discussed below; to assist in ensuring that the right environment is created that will foster the proper behaviors and a risk culture that embraces ERM.

ER 5.01 (a) Risk Ownership

This Risk Framework establishes that the CEO and the Executive Management Team are the ultimate owners of risks across JDIC. As stated elsewhere in the policy, a Risk Owner is the person that will be held ultimately responsible if a risk were to materialize and there was a loss to the JDIC.

The CEO and the Executive Management Team are responsible for ensuring that all key risks in their areas of responsibility are properly managed (mitigated, prevented, avoided transferred or accepted).

ER 5.01 (b) Risk Appetite Revisited

JDIC's risk appetite will provide the CEO and the Executive Management team, the boundaries in which risk decisions should be made. This will determine the behaviors and actions required to manage risks within the levels that JDIC is comfortable.

ER 5.01 (c) Communication

Each staff member across JDIC is encouraged to identify and bring any item that he or she believes is a risk that should be added to JDIC register. Each staff is empowered to communicate the nature of such risks to their immediate Supervisor or directly to the Risk Manager or his or her designee through email or other written means

There will be a system of governance (see **ER3.01** above) that will require risk information to be discussed at the highest levels (the CEO, the ERMC and the Board level Committees) and monitored until the risks are disposed or addressed in a satisfactory manner.

ER 5.01 (d) Performance and Rewards

JDIC will integrate the risk responsibilities of each staff member into its performance management systems, to the extent that they exist. Individuals will therefore be rewarded or penalized based on the extent to which they discharge their risk management functions.

ER 5.01 (e) Training and Human Resource Planning

The Human Resources (HR) Manager or the responsible party, in conjunction with the Risk Manager, is required to ensure that all relevant training is provided to all stakeholders so that they understand their risk management responsibilities.

The responsible HR person is also to ensure that where relevant all job descriptions are updated to reflect new and changing roles of various persons as it relates to risk management as well as to develop and recommend sanctions and commendations for those individuals who meet or fail to meet their risk management responsibilities. The HR persons responsible should include and emphasize the importance of risk management to new staff members as part of their orientation.

This Page Intentionally left Blank

ER 6. APPENDICES

i. IMPACT & LIKELIHOOD DEFINITIONS

IMPACT DEFINITIONS

Table 1

	FINANCIAL	OPERATIONAL	REPUTATIONAL	Health, Safety & Environment
DESCRIPTIONS →	**Total $ impact on JDIC OVER NEXT 18 MONTHS**	**Impact on the ability to sustain operations**	**Impact on the way stakeholders regard JDIC & its management**	**Impact on the well-being of any stakeholder (e.g., employees, public…)**
5 SIGNIFICANT	>XX	Widespread or long-term shut down of operations	Event results in sustained, serious loss in stakeholder confidence, management and board image, and market share	• Massive or sustained HSE breach • Multiple preventable fatalities or widespread illness
4 VERY HIGH	>XX	Significant, sustained operational issue	Event has a major impact on stakeholder confidence that damages company image that leads to a decline in market share.	• Significant H&S regulation violations • Single preventable Fatality • Strong punitive reaction
3 HIGH	>XX	Moderate operational challenge in size or duration	Event has a significant impact on stakeholder confidence that is challenging to regain	• Moderate HSE incident • Moderate punitive reaction
2 MODERATE	>XX	Modest operational inefficiency or situation	There is a modest, localized impact on company image and stakeholder confidence that fades over time	• Minor HSE incident • No/minor punitive reaction
1 LOW	>XX	Small operational	Event has limited, localized impact on company image	• Low significance incident

LIKELIHOOD DEFINITIONS

Table 2

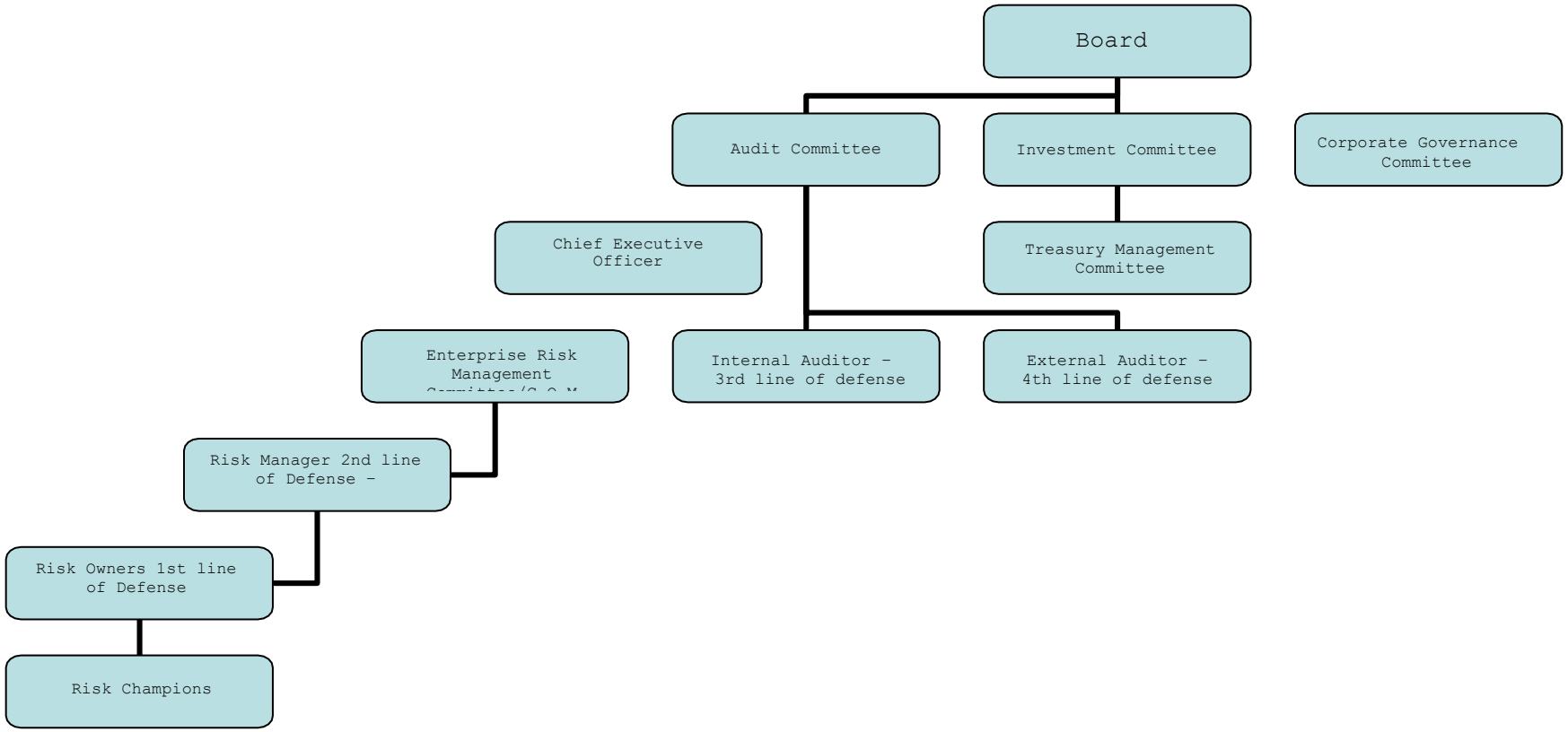
Likelihood	%	Factors to consider for Likelihood
5 VERY LIKELY	80 – 100%	• Maturity/complexity of the process or system • Past occurrences of the risk event • External factors (economic, competitive, demand for education) • Experience of management / employees • Performance indicators / industry Trends • Regulatory and governmental changes • Recent audit reports • Effectiveness training • Adherence to policies & procedures
4 HIGHLY LIKELY	60 – 79%	
3	40 – 59%	
2 UNLIKELY	20 – 39%	
1 VERY UNLIKELY	0 – 19%	

ii. RISK RESPONSE MATRIX

Table 1: Summary of Risk Actions Based on JDIC's Risk Appetite/Tolerance:

RESIDUAL RISK RATING	TARGET RISK RATING (i.e. based on JDIC's Risk Appetite or the amount of risk exposure JDIC is prepared to tolerate)	RISK RESPONSE: CORRECTIVE ACTIONS
If a risk is rated as Very High, a Risk Response should be raised	Generally, actions should be taken to reduce the risk exposure to at least Moderate or Low	These include one or more combinations of risk prevention, mitigation, avoidance or risk transfer.
If a risk is rated as High a Risk Response should be raised	Generally, actions should be taken to reduce the risk exposure to at least Moderate or Low	These include one or more combinations of risk prevention, mitigation, avoidance or risk transfer.
If a risk is rated as Moderate a Risk Response should be raised	Generally, actions should be taken to reduce the risk exposure to at least Low depending on the nature and the cost to manager or treat the risk	These include one or more combinations of risk prevention, mitigation, avoidance or risk transfer.
If a risk is rated as Low	No action is required except to monitor the risk trend	No action is required except to monitor the risk trend

iii. RISK GOVERNANCE & OPERATIONAL STRUCTURE



iv. DOCUMENT CONTROL LOG

Policy Version Number	Details of Review	Date of Review/ Approval
Version 1.0	ERM Policy and Framework drafted and approved for implementation	January 2019
Version 1.2	Review of ERM Policy and Framework conducted by the Risk Manager - Policy deemed relevant, no revisions were required.	November 29, 2022
Version 1.2	Name of Committee changed to Enterprise Risk Management Committee to better reflect its mandate.	September 7, 2023