JAMAICA SOCIAL INVESTMENT FUND ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK

Contents

ER1 ERM Policy

General

1.01 Enterprise Risk Management (ERM) is the systematic application of management policies, procedures and practices to establish the context, identify, analyse, evaluate, treat, monitor and communicate risk.

1.02 Risk is the probability of an event occurring that could have an adverse or positive impact on the achievement of established objectives of an organization.

1.03 This ERM policy demonstrates the commitment of Jamaica Social Investment Fund (JSIF) to the adoption, introduction and implementation of an effective risk management system throughout the Entity.

1.04 The ERM policy and framework address the ***general*** approach that should be used to manage the seven (7) principal categories of risks faced by the entity i.e., ***strategic***, ***reputational***, ***operational***, ***financial, ,regulatory/compliance, project implementation and environmental*** risks.

1.05 This ERM policy and framework is also therefore supplemented by more ***specific*** risk and internal control procedures in place such as those over financial risk (e.g. relating to managing funds from funding agencies), operational risk (e.g. JSIF's management of IT system failures), strategic risk (e.g. procedures in place to ensure plans are in alignment with Vision 2030), reputational risks (e.g. procedures in place to ensure funds are earmarked for projects are used appropriately), regulatory/compliance risk (e.g. those relating to complying with the Government of Jamaica standards, codes and regulations) and environmental risk (e.g. projects undertaken by the JSIF are environmental friendly). These separate policies and procedures are supplementary to this ERM policy and framework and together provide a comprehensive picture of how the entity manages risk on an enterprise basis.

1.06 The entity's risk management system is guided by the key requirements of the Committee of the Sponsoring Organization of the Treadway Commission (COSO)[1] and the ISO 31000 risk management standards.

1.07 The entity's ERM framework outlines ***risk strategy*** (risk appetite and method for assessing risks), ***risk infrastructure*** (governance and operational structures, tools, roles and responsibilities relating to risk management), ***risk analysis*** (risk identification, assessment, risk response and risk monitoring) and ***risk culture*** (attitudes and behaviors towards risks) that will be required to ensure the requirements of the risk management policy are achieved.

1.08 Definitions - see Appendix I for definitions of key terms used throughout this document.

[1] An integrated framework which provides a sound basis for establishing risk and internal control systems and determining their effectiveness.

2.0 Policy Statement

Jamaica Social Investment Fund is committed to the continuous improvement of its risk management systems and to ensure that it performs regular risk assessments of its key objectives and major change initiatives e.g. implementation of major IT systems. Every employee within the entity is responsible for the effective management of risk and the implementation of risk reduction strategies.

3.0 Policy Objectives

The objectives of the risk management policy are to:

- Provide an ERM framework;
- Identify and respond to risks affecting business objectives;
- Incorporate risk management into the strategic planning process and daily operations;
- Promote an awareness of the implications of risk management failures; and
- Embed risk management practices and principles within the culture of the organisation.

4.0 Scope

4.01 This policy is applicable to all employees within the Jamaica Social Investment Fund. The entity is required to adopt this Framework, in accordance with the type and scale of its activities and local regulatory requirements under the direction of the management team and Board. All risk management activities are subject to oversight by the Audit Committee (AC) and the Board of Directors.

5.0 Statutory Requirements

Jamaica Social Investment Fund is committed to meeting all applicable regulatory risk management requirements from all regulatory and legislative bodies.

ER2 ERM FRAMEWORK

Framework Overview

The framework comprises four pillars, namely:

- ***Risk strategy*** which covers how the entity plans to manage risk in terms of its appetite for risk and criteria for ranking risks;
- ***Risk infrastructure*** which addresses how the entity will oversee (governance) and embed (operationalize) risk management in daily operations and the strategic planning process;
- ***Risk analysis*** which captures the entity's method of risk identification, assessment, response and ongoing risk monitoring; and
- ***Risk culture*** which covers methods JSIF will use to influence the right risk behaviours within the entity.

ER3 ERM FRAMEWORK: RISK STRATEGY

Risk Appetite

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

> *With respect to all risk categories, excluding **strategic risk**, Jamaica Social Investment Fund declares its risk appetite as ranging from low to moderate, as defined in the Detailed Risk Appetite Framework (see Appendix VI. With regard to **strategic risk**, and having regard to the complex external arena within which the entity operates, JSIF's Board declares that it is willing to take risk, on a considered basis, between **moderate** and **high** but not at levels which would be considered to impose **significant** risk to the entity.*

As a general rule, JSIF's risk appetite requires the implementation of action plans that seek to reduce residual risks[2] that have been rated above Moderate (i.e. Very High or High) to at least Moderate or Low. See Appendix VI (Risk Appetite Framework) which details the specific risk appetite statements for each category of risk affecting the entity.

Risk Tolerance

Risk tolerance is effectively the same as risk appetite but taken from the opposite perspective. For example, if JSIF has a Very High Regulatory risk (e.g. "JSIF may not comply with the Government of Jamaica standards, codes and regulations"), then according to JSIF's risk appetite, it must reduce this exposure to Low (unless there are certain special circumstances that would suggest otherwise) given that the entity has a low risk tolerance for Regulatory risk exposures.

The foregoing could be expressed in the language of risk tolerance by saying "the entity will only tolerate risks relating to Government of Jamaica standards, codes and regulations," that are rated as Low.

Risk Assessment Criteria

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

JSIF 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. *Risks that could be catastrophic but are deemed Very Unlikely to happen should be subjected to further evaluation such as simulation testing and scenario analysis.*

Appendix III provides further details on the factors that the entity takes into consideration in determining impact severity and the likelihood of a risk occurring.

---

2 Residual risk refers to the amount of risk exposure that is left after taking into consideration existing control measures and other mitigating factors.

Risk Map

Appendix III also shows the entity's illustrative risk map, which is a convenient way of summarizing the risk ratings that result from the combinations[3] of likelihood and impact for a particular risk event.

Risk Responses

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

Risk Responses: Timeliness

The higher the rating of a risk, the quicker the entity 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.

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 monthly Board meetings and bimonthly meetings of the Audit Committee (AC).

H: **High Risk**; action is required by **management** within **a month,** 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 monthly board meetings and the AC.

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 treatments is to be reported at monthly board meetings and the AC.

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

Risk Responses: Corrective Actions

Generally, the entity 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 Analysis 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 by the risk owner (with support from the Risk Officer) to the board. The AC also will review the risks being recommended for risk acceptance on a quarterly basis and provide additional challenge or agreement that the risks should be accepted. The Risk Officer will coordinate and consolidate all such risks being recommended for acceptance by the entity. The risk

[3] The combinations of the Likelihood and Impact of a risk occurring

acceptance document should include a cost benefit analysis and a recommendation to accept the risk.

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 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; and
- The formal recommendation to accept the risk should form a part of the Risk Owner's report to the CEO and the Board.

ER4 ERM FRAMEWORK: RISK INFRASTRUCTURE

General Overview

This section of the framework covers the governance structure that is required to oversee the management of risk within JSIF, as well as the operational structure (management level) that is required to embed ERM in the strategic planning process and 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.

Three Lines of Defense

The roles and responsibilities of management (the operational structure) can also be viewed through the lens of the "three lines of defense". The first line of defense is line management who are required to identify, assess and monitor risks; the second line, which comprise the risk and compliance officers who work with first line to monitor and provide independent challenge to line management as to whether they are running the business within established risk appetite; and the third line, which are the internal auditors who provide independent assurance that the risk management policies and procedures are being followed. This ERM framework is built on the foundation of the three lines of defense as it is critical that these lines are strong in order to ensure a sound basis for the execution of the day to day risk management responsibilities.

Risk Governance and Operational Structures

Risk Governance Structure

The governance portion of the infrastructure deals with how the risk oversight role of the entity would be executed by the Board Committees. The Audit Committee (AC) would be the primary risk oversight Committee, overseeing the activities of the Executive Risk Management Committee (ERMC) - see Appendix II for further details.

Risk Operational Structure

The operational structure portion which is graphically depicted in Appendix II deals with management, who will be responsible for the daily execution and management of risk within the entity.

ERM Roles & Responsibilities

The roles and responsibilities include but are not limited to the areas outlined below.

Risk Governance (Oversight) Structure:

Audit Committee:

The principal functions of the Audit Committee are:

1. Serve as an independent and objective party to monitor the Entity's financial reporting process and internal financial and business control systems;
2. Review the effectiveness of the overall process for identifying and managing principal business risks and adequacy of the related disclosure;
3. Monitor the integrity of the financial statements of the company including its monthly and annual reports, and any other special financial reports to funding agencies and government entities.
4. Review the effectiveness of the overall process for ensuring regulatory and legal compliance;
5. Review and assess the audit findings of the Entity's external and internal auditors;
6. Provide an open avenue for communication amongst the external auditors, Management, the internal auditors and the Board;
7. Oversee, review and monitor the Enterprise Risk Management Framework;
8. Review and ensure the clarity and completeness of financial statements / reports, ensure that the appropriate disclosures have been made, that all material information have been presented related to audit and risk management.
9. Review the company's funding arrangements to ensure the compliance with loan agreements, memoranda of understanding and other legal requirements.

Specific Risk Functions:

Internal Control and Risk Management Systems

1. Keep under review the Entity's internal financial controls systems that identify, assess, manage and monitor financial risks, and other internal control and risk management systems;
2. Consider and challenge where necessary the effectiveness of the Entity's internal control system, including information technology security and control;
3. Understand the scope of Internal and External Auditors' review of internal control over financial reporting, and obtain reports on significant findings and recommendations, together with Management's responses; and
4. Obtain reports from management on the Very High risks within JSIF and the status of mitigating actions to reduce those risk exposures

Risk Operational (Execution) Structure

Specific Roles and Responsibilities:

The specific risk roles and responsibilities of the senior management team include but are not limited to the areas outlined below.

Managing Director

1. Provides visible support to the ERM process and ERM initiatives;
2. Supports the Chair of the ERMC (if he elects not to chair the ERMC), by attending the ERMC meetings where necessary;
3. Considers risks i.e. ensures that a strategic risk assessment of the key strategic objectives and the related strategic initiatives are done when evaluating the strategic direction of the entity; and
4. Works closely with the Risk Officer in understanding and monitoring the status of risk responses for Very High and High risks as well as close monitoring of risk with potentially Significant or High impact[4] but for which the mitigating controls are deemed to be strong or effective
5. Ensure that the Risk Officer has the right tools and resources to carry out the work.

[4] See Appendix III for definitions of Significant and High impact

Executive Risk Management Committee (ERMC)

The risk management responsibilities of this committee shall include, but not be limited to:

1. The Committee is chaired by the Managing Director or such other person as the Managing Director may nominate and the members include senior managers (i.e. department heads).
2. Discuss common risk issues and themes identified at least quarterly using the risk registers generated by the risk owners;
3. Ensures that the Risk Owners (department heads) have up to date Risk Registers, that reflect existing and emerging risks;
4. Monitors the status of action plans (risk responses) that are meant to address Very-High and High-risk exposures through challenging and requesting updates from the risk owners on the status of risk mitigating actions
5. Recommends which risks should be given priority in terms of budgets and implementation timelines
6. The Committee's deliberations provide and shape the content of the risk report and profile that is collated and submitted by the Risk Officer and submitted to the AC.

Risk and Compliance Officer

High level summary of the roles and responsibilities of the Risk Officer are as follows:

1. The Risk Officer will consolidate the risk registers received for each department to produce an entity risk profile;
2. The Risk Officer shall schedule and coordinate quarterly risk validation sessions as the means to challenge the content, accuracy and currency of the risk registers for each department;
3. Risk Officer shall perform periodic risk reviews i.e. spot checks on mitigating controls over risks that have a Significant (5) or Very-High (4) impact on the entity;
4. Risk Officer shall support risk champions/owners in updating their department's risk registers;
5. The Risk Officer will review internal audit reports – to confirm the strength of internal controls over high risk areas that could have major adverse impact on the entity;
6. The Risk Officer will coordinate the development and maintenance of a loss events and "near misses" database for the entity; and
7. The Risk Officer will prepare a consolidated report on the overall status of risk responses to mitigate Very High and High risks for monthly reporting to the Managing Director, the Board, and the AC.

Risk Owners (Department Heads)

1. Risk Owners[5] are responsible for ensuring that at least on a quarterly basis, new and existing risks for their departments are updated in their risk registers, all risks are assessed, risk responses are developed, and risk responses are monitored until the risk exposure falls within the entity's risk appetite. Risk owners (with the support of their risk champions) also have responsibility for logging loss events and near misses in the tool/template provided by the Risk Officer;
2. Select risk champions (see section below) who will assist in carrying out all relevant risk management duties that fall on the risk owner. These risk champions will also work closely with the risk owners while completing their duties;
3. It is the responsibility of the Risk Owners to ensure that all risks are responded to or treated whether the Risk Owners have the technical ability to carry out the risk treatment;
   i. For example, if a third-party IT supplier is requested to implement a new release of a software that will

[5] 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 entity. Risk Owners are ultimately the department heads. They are responsible for ensuring that all key risks in their areas of responsibility are properly managed (mitigated, prevented, avoided, transferred or accepted).

reduce exposures to known bugs in the payroll application, it is the responsibility of the risk owner (Accountant), to ensure that the entity gets the benefit of the appropriate 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.

Risk Champions (for Departments)

The roles and responsibilities of the risk champions:

1. Risk Champions for departments are nominated by the Risk Owners to assist the Risk Owners with executing their risk management duties, in accordance with the requirements of the ERM Risk Policy & Framework. It is possible 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 ERM Policy and Framework; and
3. While the Risk Champions are expected to assist the Risk Owners, ultimate responsibility for ensuring that risks are managed in accordance with the ERM Policy & Framework, rests with the Risk Owners.

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, with an impact score of 4 or 5 to assist with ensuring the mitigating controls are in fact effective. Accordingly, the Audit Plan of the Internal Audit function should be guided by the risk registers.

A limited percentage of risks rated High or Very High should also be contemplated by the Internal Audit function for inclusion in their audit plan. These audits would likely be more of a consulting nature, where Internal Audit is providing advice on the design of the internal controls that are meant to mitigate the High and Very High-risk exposures. Additionally, Internal Audit may include these risks in their audit plan, with a view of independently establishing the extent to which existing internal controls may be ineffective and therefore to also help to establish the attendant treatment required to reduce the risk exposures.

Internal Audit is required to develop their risk-based audit plan, using the results of the risk assessment[6] that is based on the requirements of the ERM policy and framework.

Additional responsibilities of the Internal Audit function include:

- Internal Audit is required to perform periodic independent checks to ensure the ERM process is working as intended and make recommendations for improvements;
- Internal Audit is required to supply all final internal audit reports to the respective Board Committees, so that they may analyze risk trends and the effectiveness of internal controls over key risk areas;
- Internal Audit may be consulted by the Risk Owners in discussions surrounding the development of risk response plans/controls that are expected to mitigate, transfer, accept, avoid or transfer major risks; and
- 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). 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.

---

6 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 the entity to be acceptable.

ERM Technologies

JSIF recognizes the importance of using appropriate technologies to support the ERM process. Consequently, the entity 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 response
4. Risk monitoring

ER5 ERM FRAMEWORK: RISK ANALYSIS

This section covers the steps that constitute the ERM risk assessment and control process; this process includes risk identification, assessment, risk response, and risk 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 departmental and operational levels which cover the business processes in the entity. Together these risks encompass the Risk Universe. Each risk (barrier) is further classified under one of the 7 categories of risks to which the entity is exposed:

1. Strategic
2. Financial
3. Operational
4. Reputational
5. Regulatory/Compliance (including Data Protection)
6. Project Implementation
7. Environmental

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

Strategic Planning Level

i. *Quarterly*
When the strategic objectives and the related strategic initiatives to achieve the objectives change, the Risk Officer will coordinate the identification of risks that affect the strategic objectives by providing support to the Risk Owners who own the execution of the various strategic objectives. Risk owners are also required to formally update the risks affecting strategic objectives in their strategic Risk Registers on a quarterly basis.

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.

Departmental level

i. *Periodically (at least quarterly)*
- Each risk owner is required to formally update the risks affecting the department in their Risk Registers periodically (quarterly).
- Addition and removal of risks should be formally reported by the Risk Owners to the board and the AC in the periodic reports submitted by the Risk Officer.

ii. *Ad Hoc*
For new risks identified based on ongoing changes affecting the department, these should be updated as they occur by the Risk Owners.

Operational level[7]

i. *Periodically (at least quarterly)*
   - Risk Owners are required to formally update the risks affecting key business processes in their Risk Registers periodically (quarterly).
   - Addition and removal of risks should be formally reported by the Risk Owners to the board and the AC in the periodic reports submitted by the Risk Officer.

ii. *Ad Hoc*
   For new risks identified based on ongoing changes affecting business processes or the environment, these should be updated as they occur.

Risk Taxonomy

Risk taxonomy addresses the basic profile of each risk that falls within the registers and the sequence with which the risk identification and assessment of a risk should be done. The sequence is very important – for example, it is very important that the risk identification and assessment start with a business objective given that the objective is what could fail if the risk event materializes. The risk taxonomy to be used (this is not an exhaustive list and could change in the future) as captured in the standard Risk Register template is as follows:

- Objective (whether it is a strategic objective, department level objective or a business process objective)
- Risk description
- Risk Category: Each risk will fall into one of 7 categories (see section 1 for further details)
- Financial (dollar value) impact of the risk
- Impact Type: the severity of the impact if the risk materialized
- Likelihood: how likely it is for a risk to materialize based on existing controls
- Root cause or contributing factor of a risk occurring
- Risk Owner
- Current Residual Risk[8]
- Target Residual Risk
- Planned Risk Response
- Budget needed to mitigate or respond to the risk
- Risk Trend

Assess Risk

After the risks have been identified at the strategic, department or business process level, the risks will then be assessed to prioritize (i.e., given a rating of Very High, High, Moderate or Low) their importance.

The entity will assess the risks by the **likelihood** of the risks occurring in the next 12 to 18 months and the **impact** of the risks if they should occur in this timeframe. The minimum requirement for "impact" is a qualitative impact assessment of the risk on the entity.

Impact should also be assessed quantitatively where it would not require an unreasonable amount of effort to do so. Financial risks (credit, liquidity, market) tend to lend themselves more readily to quantification and as far as possible

[7] This means business processes performed in the functional areas across the entity
[8] Residual Risk - Risk exposure remaining after consideration of mitigating controls and other factors

these risk exposures should be quantified, if it is deemed necessary to do so based on the size of the underlying financial assets held. Operational, reputational and certain other types of risks may be difficult to quantify, and, in these instances, the minimum requirement is a qualitative assessment, and where possible should be supplemented by a quantitative assessment.

See Appendix III for further details on the financial and non-financial considerations to be used in determining the impact and likelihood of a risk.

Timing of Risk Assessments:

i. Every six (6) months
The Risk Officer will coordinate the risk validation sessions twice yearly. To facilitate the validation session, the Risk Owners are required to update their registers in preparation for the validation sessions.

ii. Major projects, major third-party relationships etc.

- This ERM Framework requires the completion of detailed risk assessments for all major projects (e.g. new IT systems) and that these risks be monitored, and appropriate interventions employed on an ongoing basis. The project sponsors (Risk Owners) are responsible for ensuring the detailed risk assessments are completed. The relevant project management personnel should also provide project management support to assist with guiding the monitoring and successful implementation of the projects / products.
- 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 Internal Audit unit, in a consultative capacity, to be involved at all stages in all major projects / new products in order to assist in ensuring that key controls are in place to mitigate key risk factors.

Risk Response

Once the entity 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 the entity's risk appetite by the Risk Owners. The basic objective of the risk management process is to reduce unacceptable risk exposures to acceptable levels; generally, this is a rating of Low or Moderate. This will therefore require the allocation of budgets in some instances to respond to the risk, while in other instances a risk mitigation can be achieved without actual hard costs being incurred.

Risk Appetite

As stated in section 2 (Risk Strategy) and Appendix VI detailed risk appetite framework), risk appetite is set on a principle basis. The basic principle is that the entity will generally not accept risks that are rated Very High or High (although in some cases Very High and High risks may be tolerated) as determined by the Risk Assessment process.

Risk Response

1. Based on the entity's established Risk Appetite, all unacceptable risks (i.e., risks ratings that exceed the target risk appetite position for the category of risk) require a Risk Response to be raised to reduce the risk exposure to within the particular risk appetite target for the category of risk. 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.
2. Each department will review the cost (financial and non-financial) of responding to risks and make recommendations to the Managing Director, the AC and board for approval depending on the amount;

3. Each risk owner will report at least quarterly on the status of their Risk Responses to the board with support from the Risk Officer;
4. 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;
5. A Risk Response is not considered to be closed, until after it has been reviewed and signed off by the department heads in the quarterly risk validation sessions.

Risk Monitoring

This section involves various levels of monitoring of the risk environment to ensure that the required risk mitigating actions are being taken and that new and emerging risks are identified, assessed and then become part of the ongoing monitoring. See also Appendix II which speaks more specifically and directly to how the Board level committee discharges its monitoring and oversight role of the key risks facing the entity.

Board and Management

The Risk Officer will perform a coordinating role in the preparation of the risk reports for the board and the AC while working with the Risk Owners. The board and the AC will discuss the status of risk action plans (risk responses) that were to be implemented for Very High and High risk areas of the business.

Each department reports on the major areas of concern including all risks that could have significant impact on the operations (i.e. 4 and 5 impact risks) and the status of these action plans (including budgets and due dates for action plans) to the board and the AC.

The board and the AC should consider relevant sanctions that should be taken for long overdue risk responses that are not supported by proper explanations.

Risk Monitoring

Board Level

The AC will receive periodic (at least monthly) reports on the significant risk exposures as mentioned in the section immediately above being faced by the entity. The AC should update the Board at least twice per year using the risk reports presented at AC meetings. In general, these reports will fall into the following categories (not an exhaustive list):

- Quarterly/Monthly – Risk Response (Action Plan) Status and Required Budget for High and Very High risks
- Quarterly/Monthly – High and Very High Risks across each risk category
- Quarterly/Monthly – Risks being recommended for Risk Acceptance
- Quarterly/Monthly – Risk Trends (upwards or downwards) for Very High and High Risks
- Quarterly/Monthly – Risk Ratings that changed after an internal audit or other testing

Internal Audit

See section ER3 that describes the risk monitoring role played by the Internal Audit function.

External Scan

i. Sources such as those published by governments, or entities similar should be used in the scanning of the external environment. The Risk Officer and the Risk Owners for each department are responsible for scanning the external environment;
ii. The scan should include but not be limited to the political, social, environmental, regulatory, economic and other variables with a view of identifying new and emerging risks that the entity faces. The scan should also be within the context of emerging risks (e.g. data privacy) that could adversely affect the entity;
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.

Internal Scan

i. On a quarterly basis, the Risk Officer working with the risk owners is required 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 conducted by the Risk Owners, observations from the loss events / "near misses" databases, as well as internal control weaknesses identified in Internal Audit Reports and any other relevant reports produced;
iii. The analyses above should be discussed in the quarterly risk validation sessions with a view of identifying new or changing risks items / trends that should be added to the Risk Register and be appropriately actioned.

ER6 ERM FRAMEWORK: RISK CULTURE

Risk culture deals with how risk management is to be embraced and adopted within JSIF. A number of adjustments and initiatives are discussed below, to assist with ensuring the right environment is created that will foster the proper behaviours and a risk culture that embraces ERM.

Risk Ownership

This Risk framework establishes that the Managing Director and department heads along with their team members are the ultimate risk owners of risks being taken across the entity. Risk owners are responsible for the successes or failures of the decisions and actions that take place – risk owners typically among other activities are responsible for ensuring that risks are mitigated, prevented, avoided transferred or accepted depending on the circumstances surrounding a particular risk.

Risk Appetite Revisited

The entity's risk appetite (see Appendix VI and the earlier sections in this document) will provide the boundaries in which risk decisions should be made. This will determine the behaviours and actions required to manage risks within the levels that the entity is comfortable with.

Communication

Staff members are encouraged to bring any item that he or she believes is a risk to the attention of their respective supervisor.

There will be a system of governance (see **ER3** above) that will require risk information to be discussed at the highest levels (the Board, the Managing Director, Risk Owners and the Executive Risk Management Committee) and monitored until the risks are disposed or addressed in a satisfactory manner.

Performance and Rewards

The entity will, where it is feasible to do so, integrate the risk responsibilities of each staff member into its performance management systems, to the extent that such systems exist. Individuals will therefore be rewarded or penalized based on the extent to which they discharge their risk management functions.

Training and Human Resource Planning

The Risk Officer working closely with the human resource function and the Risk Owners is responsible to ensure that all relevant risk training is provided to all stakeholders so that they understand their risk management responsibilities. Training should also be extended to new hires as part of onboarding.

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 responsible HR persons should include and emphasize the importance of risk management to new staff members as part of their orientation.

This Page Intentionally left Blank

ER7 APPENDICES

I. GLOSSARY OF TERMS/DEFINITIONS

Enterprise Risk Management (ERM) is a process effected by an entity's Board, management and other personnel, applied in strategy setting 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 the entity undertakes risk management, including, but not limited to decisions made around the entity's risk appetite positions on risks faced by the entity.

Risk culture is the system of values and behaviours within the entity that shapes risk decisions of management and employees.

Risk infrastructure is the governance structure that is required to oversee the ERM process within the entity as well as the operational structure that is required to 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 analysis is the method used in identifying, assessing, managing, reporting and monitoring risks that could positively or negatively influence an entity objective.

Residual Risk - Risk exposure remaining after consideration of mitigating controls and other factors.

Internal Control - Measures that are designed to provide reasonable assurance regarding the achievement of 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 or **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))[9]

Manual Control Log - Used to track to ensure that amendments to the ERM policy and framework are done in a controlled manner

Three Lines of Defense are defined as follows:

i. First Line: The business line leaders – i.e. Managers and their team members 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.

[9] 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.

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 an "independent challenge" to the first line through reviewing its risk assessments and risk responses. The compliance function, where one exists, 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 and regulators, 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 an entity 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 entity is willing to accept/retain.

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

Risk Register – is a list of risks that needs 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 the entity's financial position 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 entity's strategic performance measures.

Reputational Risk -is the current or prospective risk to the entity's reputation and financial position arising from adverse perception of the entity's image on the part of customers, counterparties, or regulators.

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

Regulatory Risk – is the risk of legal or regulatory sanctions, financial loss, or loss the entity 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, credit risk rating, foreign exchange rate, index or prices or rates, or other variable. Elements of financial risks are:

- ***Credit Risk*** - is defined as the risk of financial loss if a debtor or counterparty fails to adhere to its contractual obligations to repay credit advance, in accordance with agreed terms and conditions. Credit risk primarily arises from direct lending and investment activities.

- ***Market Risk***; which is the risk to an institution resulting from movements in market prices, 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 business 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.

- Project Implementation Risk – is the risk of projects not being implemented properly and in accordance with donor requirements and expectations.

- Environmental Risk – is the risk of breaching compliance with environmental agreements as well as factors that impact the sustainability of JSIF projects (in the context of projects and grant funding)

II. RISK GOVERNANCE & OPERATIONAL STRUCTURE

III. IMPACT & LIKELIHOOD DEFINITIONS & RISK MAP

IMPACT DEFINITIONS

Table 1

	FINANCIAL	OPERATIONAL	REPUTATIONAL	Health Safety & Environment
DESCRIPTIONS	**Total $ impact on JSIF OVER THE NEXT 12 to 18 MONTHS**	**Impact on the ability to sustain operations**	**Impact on the way stakeholders regard JSIF**	**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 HIGH	> XX	Major sustained operational issue	Event has a major impact on stakeholder confidence that damages entity image that leads to a decline in market share	• Major H&S regulation violations • Single preventable fatality • Strong punitive reaction
3 MODERATE	> XX	Moderate operational challenge in size or duration	Event has a moderate impact on stakeholder confidence that is challenging to regain	• Moderate HSE incident • Moderate punitive reaction
2 LOW	> XX	Low operational inefficiency or situation	There is low localized impact on the entity's image and stakeholder confidence that fades over time	• Low impact HSE incident • Low punitive reaction
1 INSIGNIFICANT	> XX	Very small operational inefficiency	Event has limited, localized impact on the entity's image	• Very low impact 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 LIKELY	40 – 59%	
2 UNLIKELY	20 – 39%	
1 VERY UNLIKELY	0 – 19%	

RISK MAP

Table 3

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

IV. RISK RESPONSE MATRIX

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

RESIDUAL RISK RATING	TARGET RISK RATING (i.e. based on the entity's Risk Appetite or the amount of risk exposure the entity 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 are not necessarily required if the target risk rating is Moderate; if the target risk rating is Low, then action should be taken to reduce the exposure to Low depending on the nature and the cost to manage 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.

V. MANUAL CONTROL LOG

Manual Control #	Manual Version Number	Manual Owner	Date Provided	Date Updated	Date Returned
1	Version 1.0				

VI. DETAILED RISK APPETITE FRAMEWORK

RISK APPETITE STATEMENTS

PURPOSE

- This section of the ERM framework sets out the approach that is used to develop the entity's risk appetite positions for the types of risks faced by the entity.
- It covers the responsibility of the Board for risk oversight, definition of risk appetite, the impact of the macro and business environment and the articulation of the risk appetite statements.

THE BOARD & RISK GOVERNANCE

- The Board has ultimate responsibility for ensuring that the entity is directed and controlled in a manner that is consistent with sound risk management principles while the entity pursues its key business objectives and initiatives.
- The Board also has responsibility to communicate its views on risk management as well as to work with management to set the overall risk appetite for the entity.

RISK APPETITE: DEFINITION

According to COSO[10]:

Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.

This definition highlights the following important factors for the Entity:

1. The entity by virtue of its mandate to channel resources to community-based projects in the current macro and business environment, naturally takes *on* a number of key or principal risks that are inherent to its operations as follow:
    a. *Strategic*
    b. *Operational*
    c. *Financial*
    d. *Reputational*
    e. *Regulatory/Compliance*
    f. *Project Implementation*
    g. *Environmental*
2. The entity will need to determine the amount of risk exposure it is willing to accept (risk appetite) for each of the 7 categories of risks that it faces – the rest of this Appendix addresses the development of the Entity's risk appetite positions on these 7 types of risk.

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

3. The operating style and culture of the entity will be influenced and guided by its risk appetite statements, and thus these risk appetite statements will serve to increase the chances that management's behaviours and decisions will ensure that the entity's objectives are pursued within the articulated risk appetite guidelines.

JSIF's MACRO & BUSINESS ENVIRONMENT

The entity operates in a macro and business environment that impact their appetite for risk and ultimately the business objectives and initiatives they pursue. Captured below are some key external and internal trends and developments affecting the Entity.

- The Data Protection Act now effective since 2022
- Construction Costs
- Possible reduction of funding from funding agencies due to the business environment

RISK APPETITE STATEMENTS

- Given the macro and business environment described immediately above, the entity has developed risk appetite statements for the 7 categories of risks (see also page 1) that it must manage successfully while it pursues its business objectives:

Risk Appetite Statements

- The risk appetite statements below will guide the nature of the business decisions and risk mitigating actions that management need to take to ensure that risks are being managed within the stated risk appetite positions.
- The risk appetite statements will be described at two levels:
    - An overarching risk appetite statement for the entity
    - Specific risk appetite statements for each of the seven risk categories stated above

OVERARCHING RISK APPETITE STATEMENT FOR JSIF:

*"With respect to all risk categories, excluding **strategic risk**, the JSIF Board declares the risk appetite of the entity as ranging from low to moderate. With regard to **strategic risk** and having regard to the complex external arena within which the entity operates, the Board declares that it is willing to take risk, on a considered basis, between **moderate** and **high** but not at levels which would be considered to impose **significant** risk to the entity"*

INDIVIDUAL RISK APPETITE STATEMENTS FOR SPECIFIC RISK CATEGORIES:

RISK CATEGORIES	QUALITATIVE	QUANTITATIVE[11]	GENERALLY EXPECTED INTERNAL CONTROL PRACTICES TO ACHIEVE THE STATED RISK APPETITES
Operational Risk	*Low*	***Fraud:*** *Limit internal fraud losses to $XX per year* ***Technology:*** *Limit network down time to < 5 minutes per month*	• Ensuring IT systems and human resources are adequate to deliver on the demands of the business • Documenting policies and procedures over business processes and activities • Ensuring IT backup systems are in place in the event of a major system failure • Limiting opportunities for internal and external fraud • Ensuring adequate training is provided to staff • Striving for a culture of risk awareness and accountability
Regulatory / Compliance Risk	Low	*Compliance with XX% of tax laws*	• A focus on adherence to all laws, regulations and guidance applicable • Regular training and awareness of the need for adherence with laws and regulations at all levels
Strategic Risk	*Moderate to High*	X% of revenue to be in local markets	• A focus on ensuring that major strategic decisions are informed by accurate financial and other relevant information • Ensuring that strong project management tools and methods are employed so that major strategic projects are successfully implemented • Continuous scanning and assessment of the external environment, including industry trends, stakeholder needs, regulatory changes, political changes and economic trends.

[11]The entity should include specific measures and targets to track how well its adhering to the stated risk appetite position for each of its risk categories throughout this document. See examples above in the table. Additionally, ratios (KPIs) that are used by management to run the business could also be used as measurements of how well the entity is tracking and adhering to its risk appetite. These measures can be included in the tables above over the upcoming months.

RISK CATEGORIES	QUALITATIVE	QUANTITATIVE[11]	GENERALLY EXPECTED INTERNAL CONTROL PRACTICES TO ACHIEVE THE STATED RISK APPETITES
Reputational Risk	*Low*	X% of revenue on corporate social responsibility	• Performing adequate financial and operational due diligence on major third-party suppliers before forming relationships • Adhering to all regulatory and legal requirements • Performing rigorous screening and background checks for senior management positions • A focus on having a crisis communication plan to respond to any major adverse events affecting the entity's reputation • A system of scanning the external environment to monitor media (social and other media) for adverse comments about the entity
Financial Risk: *Market Risk*	**Low**	X% of investment to be in XX type of security	• Monitoring movements on underlying securities and designing the portfolio to achieve budgeted rate of return in line with the investment policy • Minimizing exposures to fluctuating currencies • Maintaining a diversified investment portfolio • Ensuring that the Board has adequate oversight of market risk and that there are adequate structures at the management level to manage market risks • Ensuring that a fit for purpose investment policy that is based on the reality of the entity's underlying financial instruments / portfolios exist and is implemented
Financial Risk: *Liquidity Risk*	**Low**	X% of total assets to be in cash or cash equivalents	For the entity to achieve "Low" residual risk exposure over liquidity risk require in general, the following internal controls to be generally practiced: • Ensuring that there is enough cash to meet short term cash and similar obligations. • Ensuring adequate funding is available to meet medium to long term operational and financial obligations

RISK CATEGORIES	QUALITATIVE	QUANTITATIVE[11]	GENERALLY EXPECTED INTERNAL CONTROL PRACTICES TO ACHIEVE THE STATED RISK APPETITES
Project Implementation	**Low**	X% of projects not completed on time and within budget	For the entity to achieve "Low" residual risk exposure over project implementation risk require in general, the following internal controls to be generally practiced: • Strict adherence project management best practices • Systems with up to date material costs • Reliable vendors and contractors with a proven track record for meeting timelines.
Environmental	**Low**	0 breaches of environmental laws and regulations	• Strong knowledge of environmental regulatory requirements • Strong relationship with and involvement of environmental regulatory bodies e.g. NEPA • Sound environmental assessment before the start of any project • A focus on having a crisis communication plan to respond to any major adverse events affecting the entity's reputation

1. VERSION CONTROL

Key Information

Title	Enterprise Risk Management Policy & Framework
Prepared By	Consultant
Reviewed By	JSIFLegal, Audit Committee
Owner	JSIFLegal
Approved By	Board of Directors
Approval Date	December 10 2024
Version Number	V 1.0
Review Frequency	Annually
Next Review Date	

Revision History

Version	Date	Summary Changes	Initials	Changes Marked

Approvals: This document requires the following signed approvals.

Name/Title	Version	Signature	Date
Chair -Board of Directors	V 1.0		05-Feb-2025
Chair -Audit Committee	V 1.0		04-Feb-2025
Managing Director	V 1.0		03-Feb-2025

Distribution: This document has been distributed to

Name	Title/Division	Place of distribution	Date of Issue	Version
JSIF Staff	All departments	Intranet		V 1.0
Board of Directors				

Linked Policies/Documents

Data Privacy Workplace Policy