RISK MANAGEMENT POLICY

FOR THE

INITIATIVE FOR LEGAL AID

(ILA)

TABLE OF CONTENTS

6.15 Review of Specialized Risks

CHAPTER SEVEN: RISK MONITORING, REPORTING, BUSINESS CONTINUITY AND CRISIS MANAGEMENT

7.1 Introduction

7.2 Purpose of Risk Monitoring and Reporting

7.3 Risk Monitoring Framework

7.4 Continuous Risk Monitoring

7.5 Risk Registers

7.6 Key Risk Indicators (KRIs)

7.7 Risk Reporting Structure

7.8 Risk Escalation Framework

7.9 Incident Management

7.10 Business Continuity Management

7.11 Business Continuity Planning

7.12 Critical Functions

7.13 Business Continuity Response Levels

7.14 Crisis Management Framework

7.15 Emergency Communication

7.16 Recovery and Restoration

7.17 Lessons Learned

7.18 Audits and Independent Reviews

7.19 Risk Management Performance Review

7.20 Continuous Improvement

CHAPTER EIGHT: POLICY IMPLEMENTATION, TRAINING, COMPLIANCE, REVIEW AND AMENDMENT

8.1 Introduction

8.2 Policy Implementation Framework

8.3 Responsibilities for Policy Implementation

8.4 Risk Management Training and Capacity Building

8.5 Staff Induction

8.6 Communication and Awareness

8.7 Compliance Monitoring

8.8 Risk Management Assurance

8.9 Non-Compliance with the Policy

8.10 Documentation and Record Keeping

8.11 Confidentiality and Information Protection

8.12 Relationship with Other Policies

8.13 Policy Review

8.14 Review Frequency

8.15 Policy Amendment Process

8.16 Version Control

8.17 Effective Date

8.18 Approval

8.19 Conclusion

RISK MANAGEMENT POLICY

INITIATIVE FOR LEGAL AID (ILA)

CHAPTER ONE

INTRODUCTION AND POLICY FRAMEWORK

1.1 Introduction

Initiative for Legal Aid (ILA) recognizes that effective risk management is fundamental to achieving its mission of promoting access to justice, legal empowerment, human rights and the rule of law in the Republic of South Sudan. As a non-governmental organization operating in dynamic and often challenging environments, ILA faces a range of strategic, operational, financial, legal, security, technological and reputational risks that may affect its ability to deliver programmes and fulfil its organizational objectives.

This Risk Management Policy establishes a structured and systematic framework for identifying, assessing, managing, monitoring and reporting risks across all organizational functions. It promotes informed decision-making, strengthens internal controls, enhances organizational resilience and supports responsible stewardship of resources.

Risk management is an integral part of good governance and shall be embedded in the planning, implementation, monitoring and evaluation of all organizational activities.

1.2 Policy Statement

ILA is committed to proactively identifying and managing risks that may affect the achievement of its objectives.

The organization shall:

- Integrate risk management into strategic and operational planning;
- Promote a culture of risk awareness and accountability;
- Apply appropriate internal controls to reduce risk;
- Monitor emerging risks and respond promptly;
- Strengthen organizational resilience and business continuity;
- Comply with applicable laws, donor requirements and recognized international standards.

Risk management shall support—not hinder—innovation and informed decision-making.

1.3 Purpose of the Policy

The purpose of this Policy is to:

a) Establish a comprehensive framework for managing organizational risks;

b) Promote proactive identification and assessment of risks;

c) Strengthen internal control systems and organizational resilience;

d) Support informed and evidence-based decision-making;

e) Safeguard the organization's people, assets, finances, information and reputation;

f) Promote compliance with legal, regulatory and donor obligations;

g) Ensure continuity of critical organizational operations during disruptions.

1.4 Objectives

The objectives of this Policy are to:

- Integrate risk management into all organizational functions;
- Protect beneficiaries, staff, volunteers and partners from avoidable risks;
- Strengthen governance and accountability;
- Improve organizational preparedness for emergencies and crises;
- Enhance financial sustainability and operational efficiency;
- Support continuous improvement through regular monitoring and review;
- Foster a culture where risk management is everyone's responsibility.

1.5 Scope of Application

This Policy applies to:

- The Board of Directors;
- Executive Director;
- Senior Management;
- Employees;
- Volunteers;
- Interns;
- Consultants;
- Contractors;
- Partner organizations, where applicable by agreement;
- All programmes, projects, departments and field operations of ILA.

The Policy applies to strategic, operational and administrative activities undertaken by or on behalf of ILA.

1.6 Types of Organizational Risks

ILA recognizes that risks may arise from a wide range of internal and external factors, including but not limited to:

a) Strategic Risks

Risks affecting the achievement of organizational goals, strategic priorities or long-term sustainability.

b) Operational Risks

Risks arising from internal processes, systems, human resources or programme implementation.

c) Financial Risks

Risks relating to budgeting, fraud, financial controls, funding, liquidity, foreign exchange and financial reporting.

d) Legal and Regulatory Risks

Risks arising from non-compliance with applicable laws, regulations, contracts or donor requirements.

e) Security and Safety Risks

Risks affecting the safety and security of staff, volunteers, beneficiaries, visitors or organizational assets.

f) Information and Cybersecurity Risks

Risks relating to data protection, cybersecurity, unauthorized access, technology failures and information loss.

g) Reputational Risks

Risks that may undermine public confidence, donor trust or stakeholder relationships.

h) Programme Risks

Risks affecting programme quality, implementation, safeguarding, beneficiary protection, partnerships or achievement of intended results.

i) Environmental and Climate Risks

Risks arising from environmental degradation, natural hazards or climate-related events that may disrupt operations.

j) Political and Contextual Risks

Risks arising from conflict, political instability, civil unrest, policy changes or humanitarian emergencies.

1.7 Guiding Principles

Risk management within ILA shall be guided by the following principles:

- Integration into all organizational processes;
- Accountability at all levels;
- Proportionality of risk responses;
- Transparency and effective communication;
- Evidence-based decision-making;
- Continuous improvement;
- Protection of beneficiaries and staff;
- Compliance with applicable legal and donor requirements;
- Respect for ethical standards and human rights.

1.8 Relationship with Other Policies

This Policy shall be read together with:

- Finance and Accounting Policy;
- Procurement and Asset Management Policy;
- Human Resource and Administration Manual;
- ICT Policy;
- MEAL Policy;
- PSEAH Policy;
- Anti-Fraud, Corruption and Whistleblowing Policy;
- Code of Conduct and Ethics Policy;
- Any other policies adopted by ILA.

Where risks relate to matters governed by another policy, the relevant policies shall be applied in a complementary manner.

1.9 Policy Ownership

The Board of Directors has overall responsibility for risk governance.

The Executive Director shall ensure implementation of this Policy, while every manager, supervisor and staff member shares responsibility for identifying, reporting and managing risks within their areas of responsibility.

Risk management is a collective responsibility and shall form part of everyday decision-making throughout the organization.

1.10 Effective Date and Review

This Policy shall become effective upon approval by the Board of Directors of Initiative for Legal Aid (ILA).

The Policy shall be reviewed every **three (3) years**, or earlier where required due to changes in organizational structure, operational context, legal requirements or donor expectations.

CHAPTER TWO

DEFINITIONS, INTERPRETATION AND ACRONYMS

2.1 Introduction

This Chapter provides the definitions, interpretation rules and acronyms used throughout this Risk Management Policy. The purpose of this Chapter is to ensure a common understanding of key risk management concepts and to promote consistent application of the Policy across all organizational functions.

Unless the context otherwise requires, the following terms shall have the meanings assigned to them below.

2.2 Definitions

2.2.1 Risk

Risk means the possibility that an event, action or circumstance may occur and affect the achievement of ILA's objectives. A risk may have negative consequences, positive consequences, or both.

2.2.2 Risk Management

Risk Management means the coordinated activities undertaken to identify, assess, evaluate, treat, monitor and report risks in order to support the achievement of organizational objectives.

2.2.3 Enterprise Risk Management (ERM)

Enterprise Risk Management means an integrated organization-wide approach to managing risks across all functions, programmes, projects and operations.

2.2.4 Risk Appetite

Risk Appetite means the amount and type of risk that ILA is willing to accept in pursuit of its objectives.

2.2.5 Risk Tolerance

Risk Tolerance means the acceptable level of variation or exposure that ILA is prepared to withstand for a particular risk.

2.2.6 Inherent Risk

Inherent Risk means the level of risk that exists before any controls or mitigation measures are applied.

2.2.7 Residual Risk

Residual Risk means the level of risk remaining after existing controls or mitigation measures have been applied.

2.2.8 Risk Owner

Risk Owner means the individual or department responsible for managing, monitoring and reporting a specific risk.

2.2.9 Risk Register

Risk Register means a formal record of identified risks, their assessment, existing controls, mitigation measures, responsible persons and review dates.

2.2.10 Risk Assessment

Risk Assessment means the process of identifying risks and evaluating their likelihood and impact.

2.2.11 Likelihood

Likelihood means the probability that a risk event will occur.

2.2.12 Impact

Impact means the extent of the consequences that may result if a risk event occurs.

2.2.13 Risk Rating

Risk Rating means the overall level of risk determined by considering both likelihood and impact.

2.2.14 Control

Control means a policy, procedure, process, practice or action designed to prevent, detect or reduce a risk.

2.2.15 Mitigation

Mitigation means the action taken to reduce the likelihood or impact of a risk.

2.2.16 Risk Treatment

Risk Treatment means the process of selecting and implementing measures to modify a risk.

2.2.17 Strategic Risk

Strategic Risk means a risk that may affect the achievement of ILA's long-term objectives, mission or strategic priorities.

2.2.18 Operational Risk

Operational Risk means a risk arising from internal processes, systems, people or day-to-day operations.

2.2.19 Financial Risk

Financial Risk means a risk relating to budgeting, funding, cash flow, financial controls, fraud, accounting or financial reporting.

2.2.20 Compliance Risk

Compliance Risk means a risk arising from failure to comply with laws, regulations, donor requirements, contracts or organizational policies.

2.2.21 Reputational Risk

Reputational Risk means a risk that may damage public confidence, donor trust, stakeholder relationships or the reputation of ILA.

2.2.22 Security Risk

Security Risk means a risk that may affect the safety and security of staff, volunteers, beneficiaries, visitors, assets or operations.

2.2.23 Safeguarding Risk

Safeguarding Risk means a risk of harm, exploitation, abuse, neglect or harassment affecting beneficiaries, staff or other stakeholders.

2.2.24 Incident

Incident means an event that has occurred and has caused, or could have caused, harm, loss, damage, disruption or breach of organizational requirements.

2.2.25 Near Miss

Near Miss means an event that could have resulted in harm or loss but did not do so due to chance or timely intervention.

2.2.26 Business Continuity

Business Continuity means the ability of ILA to continue delivering critical functions during and after a disruption.

2.2.27 Crisis

Crisis means a significant event or situation that threatens the safety, operations, reputation or viability of ILA and requires urgent coordinated response.

2.2.28 Key Risk Indicator (KRI)

Key Risk Indicator means a measurable value used to monitor changes in risk exposure.

2.2.29 Internal Control

Internal Control means a process designed to provide reasonable assurance regarding the achievement of organizational objectives.

2.2.30 Stakeholder

Stakeholder means any individual, group or organization that may affect, be affected by, or have an interest in ILA's activities.

2.3 Interpretation

In this Policy, unless the context otherwise requires:

- The word "shall" indicates a mandatory requirement.
- The word "should" indicates a recommended practice.
- The word "may" indicates discretion.
- Words importing the singular include the plural and vice versa.
- References to any law include amendments or replacements of that law.
- References to departments include programmes, projects and field offices where applicable.
- Headings are included for convenience and do not affect interpretation.

2.4 Acronyms and Abbreviations

Acronym	Meaning
BOD	Board of Directors
ERM	Enterprise Risk Management
ILA	Initiative for Legal Aid
ICT	Information and Communication Technology
KRI	Key Risk Indicator
MEAL	Monitoring, Evaluation, Accountability and Learning
PSEAH	Prevention of Sexual Exploitation, Abuse and Harassment
SOP	Standard Operating Procedure

2.5 Consistent Use of Terms

The definitions contained in this Chapter shall be applied consistently throughout this Policy and, where relevant, across other ILA governance and operational policies.

CHAPTER THREE

RISK MANAGEMENT GOVERNANCE, LEADERSHIP AND INSTITUTIONAL RESPONSIBILITIES

3.1 Introduction

Effective risk management is dependent upon sound governance, strong leadership and clearly defined responsibilities. Risk management is not the responsibility of a single individual or department; rather, it is an integral part of governance, management and day-to-day operations throughout ILA.

This Chapter establishes the governance structure through which risks shall be identified, managed, monitored and reported, ensuring accountability at every level of the organization.

ILA adopts the **"Three Lines Model"** (formerly known as the Three Lines of Defence Model), adapted for the operational realities of non-governmental organizations. Under this model:

- **First Line:** Programme and operational management own and manage risks.
- **Second Line:** Management functions provide oversight, guidance and monitoring.
- **Third Line:** Independent assurance is provided through internal audit, external audit, donor reviews or other independent assessments, where applicable.

This governance framework promotes accountability while ensuring that risk management is integrated into all organizational processes.

3.2 Risk Governance Framework

ILA's risk governance framework consists of the following institutional levels:

1. Board of Directors
2. Board Committees (where established)
3. Executive Director
4. Senior Management Team
5. Department Heads and Programme Managers
6. Project Officers and Supervisors
7. All Employees
8. Volunteers, Interns and Consultants
9. Implementing Partners and Sub-grantees (where applicable)

Each level has distinct but complementary responsibilities.

3.3 Principles of Risk Governance

The governance of risk within ILA shall be guided by the following principles:

a) Accountability

Every person shall be accountable for managing risks within their area of responsibility.

b) Leadership

Leadership shall demonstrate commitment to effective risk management through actions, decisions and allocation of resources.

c) Transparency

Risk-related information shall be communicated accurately and in a timely manner.

d) Shared Responsibility

Risk management is everyone's responsibility.

e) Continuous Improvement

Risk management practices shall be regularly reviewed and strengthened.

f) Independence of Oversight

Where independent assurance activities are undertaken, they shall remain objective and free from undue influence.

3.4 Responsibilities of the Board of Directors

The Board of Directors bears ultimate responsibility for risk governance.

Without prejudice to its wider governance responsibilities, the Board shall:

a) Governance

Approve this Risk Management Policy and any amendments.

b) Risk Oversight

Provide strategic oversight of organizational risks.

c) Risk Appetite

Approve the organization's Risk Appetite Statement and periodically review its continued appropriateness.

d) Strategic Risk Review

Review significant strategic risks at least annually or more frequently where circumstances require.

e) Internal Control

Ensure that effective internal control systems exist throughout the organization.

f) Organizational Resilience

Ensure that appropriate business continuity and crisis management arrangements are maintained.

g) Compliance

Ensure compliance with legal, regulatory and donor requirements relating to risk management.

h) Resource Allocation

Ensure that adequate financial, human and technological resources are available to support effective risk management.

3.5 Board Committees

Where the Board establishes committees such as:

- Finance and Audit Committee;
- Governance Committee;
- Risk Committee; or
- Programme Committee,

those committees shall support the Board by reviewing risks within their respective mandates and making recommendations for Board consideration.

The establishment of committees shall not diminish the collective responsibility of the Board.

3.6 Responsibilities of the Executive Director

The Executive Director is the Accounting Officer and chief executive responsible for implementing this Policy.

The Executive Director shall:

a)

Provide visible leadership in promoting a positive risk management culture.

b) Ensure that risk management is integrated into strategic planning, annual work planning and budgeting.

c) Ensure that organizational risks are regularly identified and assessed.

d) Approve organizational risk registers and ensure that they remain current.

e) Ensure implementation of appropriate mitigation measures.

f) Allocate adequate resources for risk management.

g) Ensure significant risks are reported to the Board.

h) Ensure that serious incidents are investigated appropriately.

i) Promote continuous organizational learning arising from risk events.

j) Ensure effective implementation of business continuity arrangements.

3.7 Responsibilities of Senior Management

Senior Management shall collectively provide operational leadership for risk management.

Their responsibilities include:

- Reviewing departmental risks.
- Monitoring implementation of mitigation plans.
- Coordinating cross-departmental risk responses.
- Reviewing organizational risk reports.
- Ensuring departmental compliance with this Policy.
- Escalating critical risks to the Executive Director.
- Promoting organizational learning from incidents.

Senior Management shall include risk management as a standing agenda item during management meetings.

3.8 Responsibilities of Department Heads

Every Department Head shall serve as the primary Risk Owner for risks within their department.

Department Heads shall:

a) Identify departmental risks.

b) Maintain Departmental Risk Registers.

c) Review risks regularly.

d) Ensure staff understand applicable risks.

e) Monitor implementation of internal controls.

f) Report emerging risks promptly.

g) Ensure risk assessments are completed before introducing significant new activities.

h) Implement corrective actions arising from audits and investigations.

3.9 Responsibilities of Programme Managers

Programme Managers shall ensure that risk management is integrated throughout the programme cycle.

This includes:

- project design;
- proposal development;
- implementation;
- monitoring;
- evaluation;
- project closure.

Programme Managers shall assess risks relating to:

- beneficiary protection;
- safeguarding;
- security;
- partnerships;
- donor compliance;
- financial management;
- programme quality;
- sustainability.

3.10 Responsibilities of Finance Personnel

Finance personnel shall manage financial risks including:

- fraud;
- budgeting;
- liquidity;
- donor compliance;
- financial reporting;
- taxation;
- asset protection;
- internal financial controls.

Finance personnel shall immediately report suspected financial irregularities in accordance with the Anti-Fraud, Corruption and Whistleblowing Policy.

3.11 Responsibilities of Human Resource Personnel

Human Resource personnel shall manage risks relating to:

- staffing;
- recruitment;
- employee welfare;
- disciplinary matters;
- safeguarding;
- occupational health and safety;
- staff retention;
- organizational culture.

HR shall ensure that risk awareness forms part of staff induction and ongoing training.

3.12 Responsibilities of ICT Personnel

ICT personnel shall manage risks relating to:

- cybersecurity;
- system availability;
- information security;
- data integrity;
- digital infrastructure;
- disaster recovery;
- user access controls.

ICT risks shall be managed in accordance with the ICT Policy and this Policy.

3.13 Responsibilities of Employees

Every employee shall:

- comply with this Policy;
- identify and report risks promptly;
- follow approved procedures;
- protect organizational resources;
- cooperate during investigations;
- participate in risk management training;
- report incidents and near misses;
- suggest improvements to organizational controls where appropriate.

Failure to report significant risks may constitute misconduct.

3.14 Responsibilities of Volunteers, Interns and Consultants

Volunteers, interns and consultants shall:

- comply with this Policy;
- report identified risks;
- safeguard confidential information;
- protect organizational property;
- cooperate with management during risk assessments.

Their contractual or volunteer status does not diminish their responsibility to support effective risk management.

3.15 Responsibilities of Implementing Partners and Sub-Grantees

Where required by agreement, implementing partners and sub-grantees shall:

- maintain appropriate risk management systems;
- comply with donor requirements;
- report significant risks affecting jointly implemented activities;
- cooperate during audits and assessments;
- implement agreed mitigation measures.

ILA reserves the right to assess partner risk management capacity before entering into or renewing partnership agreements.

3.16 Risk Owners

Every significant organizational risk shall have a designated Risk Owner.

A Risk Owner shall:

- monitor the assigned risk;
- ensure mitigation measures are implemented;
- review risk ratings periodically;
- report changes in risk exposure;
- maintain relevant documentation.

Designation as Risk Owner does not transfer accountability from management but clarifies operational responsibility.

3.17 Collective Responsibility

Risk management is a shared organizational responsibility.

Every person associated with ILA shall:

- remain vigilant;
- report concerns promptly;
- support implementation of controls;
- contribute to organizational resilience.

Risk management shall be regarded as an integral part of professional performance and organizational stewardship.

3.18 Accountability for Failure to Manage Risks

Failure to discharge responsibilities under this Policy may result in:

- management intervention;
- corrective action;
- performance management measures;
- disciplinary proceedings;
- contractual remedies;
- referral to competent authorities where required by law.

Any action taken shall be consistent with the Human Resource and Administration Manual, applicable contractual terms and the laws of the Republic of South Sudan.

3.19 Ethical Leadership and Risk Culture

Leaders at all levels shall foster a culture in which:

- risks are reported without fear of retaliation;
- mistakes are used as opportunities for learning;
- accountability is balanced with fairness;
- innovation is encouraged within acceptable risk limits;
- ethical conduct informs decision-making.

An effective risk culture is essential to achieving ILA's mission and maintaining the confidence of beneficiaries, donors, partners and the public.

CHAPTER FOUR

RISK IDENTIFICATION, CLASSIFICATION AND ASSESSMENT FRAMEWORK

4.1 Introduction

Effective risk management begins with the ability to identify, understand and evaluate risks before they adversely affect the achievement of organizational objectives.

ILA recognizes that risks may arise from internal and external factors and may affect strategic objectives, programme delivery, financial sustainability, legal compliance, organizational reputation, staff safety, beneficiary protection and operational continuity.

This Chapter establishes the framework through which ILA shall identify, document, analyse, evaluate and prioritize risks across all organizational functions.

4.2 Purpose of Risk Identification and Assessment

The purpose of risk identification and assessment is to:

a) Ensure that risks are recognized at an early stage;

b) Understand the causes, consequences and potential impact of risks;

c) Prioritize risks requiring management attention;

d) Support informed decision-making;

e) Determine appropriate risk treatment measures;

f) Strengthen organizational preparedness and resilience;

g) Improve accountability and internal controls.

4.3 Risk Identification Principles

Risk identification within ILA shall be guided by the following principles:

a) Comprehensive

Risk identification shall consider all relevant sources of risk, including internal and external factors.

b) Systematic

Risks shall be identified using structured methods and documented processes.

c) Continuous

Risk identification shall not be limited to annual assessments but shall occur throughout the life cycle of programmes, projects and operations.

d) Inclusive

Relevant stakeholders shall be consulted where appropriate to ensure diverse perspectives are considered.

e) Forward-Looking

Risk identification shall consider emerging risks that may affect future operations.

4.4 Sources of Risk Identification

ILA shall identify risks through multiple sources, including:

4.4.1 Strategic Planning Processes

Risks shall be identified during:

- strategic planning;
- annual planning;
- organizational reviews;
- programme design;
- resource planning.

4.4.2 Programme and Project Management

Programme teams shall identify risks during:

- proposal development;
- project inception;
- implementation planning;
- monitoring visits;
- evaluations;
- project closure.

4.4.3 Financial Management Processes

Financial risks shall be identified through:

- budgeting;
- financial reporting;
- audits;

- cash flow monitoring;
- donor compliance reviews.

4.4.4 Procurement Processes

Procurement-related risks shall be identified through:

- procurement planning;
- supplier assessments;
- contract management;
- market analysis.

4.4.5 Human Resource Processes

HR-related risks shall be identified through:

- workforce planning;
- recruitment processes;
- staff performance reviews;
- employee feedback;
- workplace assessments.

4.4.6 Monitoring, Evaluation, Accountability and Learning (MEAL)

MEAL systems shall contribute to risk identification through:

- monitoring findings;
- beneficiary feedback;
- evaluations;
- lessons learned;
- programme quality assessments.

4.4.7 Audits and Assessments

Risks may be identified through:

- internal audits;
- external audits;
- donor assessments;
- compliance reviews;
- investigations.

4.4.8 Incident Reporting

Risks shall also be identified through:

- security incidents;
- safeguarding reports;
- fraud allegations;
- data breaches;
- operational disruptions;
- complaints.

4.5 Risk Classification Framework

To ensure consistency, ILA shall classify risks into the following categories:

4.5.1 Strategic Risks

Strategic risks are risks that may affect the achievement of ILA's mission, vision and long-term objectives.

Examples include:

- failure to achieve strategic goals;
- changes in operating environment;
- funding dependency;
- loss of strategic partnerships;
- changes in government policy;
- inability to adapt to emerging needs.

4.5.2 Programme and Project Risks

Programme risks relate to the ability of ILA to successfully implement projects and achieve intended results.

Examples include:

- poor programme design;
- inadequate beneficiary engagement;
- failure to achieve indicators;
- implementation delays;
- inadequate technical capacity;
- weak partner performance.

4.5.3 Operational Risks

Operational risks arise from internal processes, systems, people or resources.

Examples include:

- ineffective procedures;
- inadequate staffing;
- equipment failure;
- administrative weaknesses;
- supply chain disruptions;
- operational inefficiencies.

4.5.4 Financial Risks

Financial risks relate to the management and protection of financial resources.

Examples include:

- fraud;
- corruption;
- inaccurate financial reporting;
- funding shortages;
- cash flow challenges;
- donor disallowances;
- tax compliance failures.

4.5.5 Legal and Compliance Risks

These arise from failure to comply with applicable requirements.

Examples include:

- violation of laws;
- breach of contracts;
- failure to meet donor obligations;
- regulatory penalties;
- inadequate documentation.

4.5.6 Human Resource Risks

HR risks relate to people management.

Examples include:

- inability to recruit qualified personnel;

- staff turnover;
- workplace disputes;
- inadequate training;
- misconduct;
- safeguarding failures.

4.5.7 Safeguarding Risks

Safeguarding risks relate to potential harm against beneficiaries, staff or stakeholders.

Examples include:

- sexual exploitation and abuse;
- harassment;
- child protection violations;
- abuse of authority;
- failure to protect vulnerable persons.

These risks shall be managed in accordance with the PSEAH Policy and relevant safeguarding procedures.

4.5.8 Security and Safety Risks

Security risks relate to threats affecting people, assets and operations.

Examples include:

- armed conflict;
- civil unrest;
- crime;
- travel risks;
- workplace accidents;
- health emergencies.

4.5.9 ICT and Information Security Risks

ICT risks relate to technology and information management.

Examples include:

- cyber-attacks;
- unauthorized access;
- data loss;
- system failure;
- malware;
- privacy breaches.

These risks shall be managed in accordance with the ICT Policy and Data Protection requirements.

4.5.10 Reputational Risks

Reputational risks relate to public confidence and stakeholder trust.

Examples include:

- negative publicity;
- ethical violations;
- poor programme performance;
- misuse of funds;
- inappropriate public communication.

4.5.11 Partnership Risks

Partnership risks arise from relationships with external organizations.

Examples include:

- weak partner capacity;
- non-compliance;
- misuse of resources;
- reputational damage;
- failure to achieve agreed objectives.

4.5.12 Environmental and Climate Risks

These include:

- natural disasters;
- climate-related disruptions;
- environmental harm;
- resource scarcity;
- changes affecting programme delivery.

4.6 Risk Identification Methodology

ILA shall use a combination of methods including:

a) Risk Workshops

Structured discussions involving relevant staff and stakeholders.

b) SWOT Analysis

Assessment of internal strengths and weaknesses and external opportunities and threats.

c) Scenario Analysis

Assessment of possible future events and their consequences.

d) Lessons Learned Reviews

Analysis of previous incidents and experiences.

e) Consultation

Engagement with staff, beneficiaries, partners and experts.

f) Data Analysis

Review of monitoring reports, audits, complaints and performance information.

4.7 Risk Assessment Process

Each identified risk shall undergo assessment through the following steps:

Step One: Describe the Risk

The risk shall be clearly documented, including:

- risk event;
- possible causes;
- potential consequences;
- affected objectives.

Step Two: Assess Inherent Risk

The risk shall first be assessed before considering existing controls.

This determines the organization's initial exposure.

Step Three: Evaluate Existing Controls

Existing measures shall be reviewed to determine whether they effectively reduce risk.

Step Four: Determine Residual Risk

The remaining risk after controls are applied shall be assessed.

Step Five: Determine Required Treatment

Appropriate mitigation actions shall be developed based on the risk level.

4.8 Risk Likelihood Assessment

ILA shall assess likelihood using the following scale:

Rating	Description	Explanation
1	Rare	Unlikely to occur except in exceptional circumstances
2	Unlikely	Could occur but not expected
3	Possible	May occur at some point
4	Likely	Expected to occur in many circumstances
5	Almost Certain	Expected to occur frequently

4.9 Risk Impact Assessment

Impact shall be assessed considering consequences relating to:

- organizational objectives;
- beneficiaries;
- finances;
- legal compliance;
- reputation;
- staff safety;
- programme delivery.

Impact scale:

Rating	Description
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Severe/Critical

4.10 Risk Rating Methodology

The overall risk rating shall be determined by:

Likelihood × Impact = Risk Rating

Example:

Likelihood: 4
Impact: 5

Risk Score:

4 × 5 = 20 (High/Critical Risk)

4.11 Risk Classification Levels

ILA shall classify risks as follows:

Low Risk

Requires routine monitoring and existing controls.

Moderate Risk

Requires management attention and periodic review.

High Risk

Requires documented mitigation measures and active monitoring.

Critical Risk

Requires immediate escalation to Senior Management and, where appropriate, the Board.

4.12 Risk Assessment Documentation

All significant risks shall be documented through:

- Organizational Risk Register;
- Departmental Risk Registers;
- Project Risk Registers;
- Risk Assessment Forms;
- Risk Treatment Plans.

4.13 Review of Risk Assessments

Risk assessments shall be reviewed:

- at least annually;
- during significant organizational changes;
- when new programmes commence;

- after major incidents;
- when operating conditions change.

4.14 Risk Escalation

Risks shall be escalated where:

- the impact is significant;
- controls are ineffective;
- mitigation actions are delayed;
- the risk threatens organizational objectives;
- urgent decisions are required.

CHAPTER FIVE

RISK TREATMENT, MITIGATION STRATEGIES AND INTERNAL CONTROL FRAMEWORK

5.1 Introduction

Risk identification and assessment alone do not protect an organization from adverse events. Effective risk management requires deliberate actions to address identified risks through appropriate treatment measures, strengthened internal controls and continuous monitoring.

Initiative for Legal Aid (ILA) shall adopt a proactive approach to risk treatment by selecting appropriate responses that reduce the likelihood and/or impact of risks while enabling the organization to achieve its strategic and operational objectives.

Risk treatment shall be proportionate to the level of risk, cost-effective and consistent with ILA's values, policies, legal obligations and donor requirements.

5.2 Purpose of Risk Treatment

The purpose of risk treatment is to:

a) Reduce exposure to unacceptable risks;

b) Strengthen organizational resilience;

c) Protect beneficiaries, personnel and stakeholders;

d) Safeguard organizational resources;

e) Improve operational effectiveness;

f) Ensure compliance with applicable obligations;

g) Support achievement of organizational objectives.

5.3 Risk Treatment Principles

ILA shall apply the following principles when determining risk responses:

a) Proportionality

The response shall correspond to the seriousness of the risk.

b) Effectiveness

Risk treatments shall address the underlying causes of risks rather than only symptoms.

c) Sustainability

Controls shall be practical, affordable and capable of being maintained over time.

d) Accountability

Every risk treatment measure shall have a responsible owner.

e) Continuous Improvement

Risk responses shall be reviewed and adjusted based on changing circumstances.

5.4 Risk Treatment Options

ILA shall use one or more of the following risk treatment approaches:

5.4.1 Risk Avoidance

Risk avoidance involves eliminating activities or circumstances that create unacceptable exposure.

Examples include:

- withdrawing from activities where risks cannot be managed;
- declining partnerships with unacceptable risk profiles;
- refusing transactions that violate ethical or legal requirements.

Risk avoidance shall be considered where potential consequences are severe and cannot reasonably be mitigated.

5.4.2 Risk Reduction or Mitigation

Risk reduction involves implementing controls and measures to decrease the likelihood or impact of a risk.

Examples include:

- improved procedures;
- staff training;
- enhanced supervision;
- strengthened documentation;
- additional security measures;
- technical safeguards.

Risk mitigation shall be the most common response for manageable organizational risks.

5.4.3 Risk Transfer or Sharing

Risk transfer involves sharing responsibility for managing a risk with another party.

Examples include:

- insurance arrangements;
- contractual provisions;
- service agreements;
- partnership arrangements.

Risk transfer does not eliminate ILA's responsibility to oversee the risk.

5.4.4 Risk Acceptance

Risk acceptance involves consciously deciding to retain a risk where:

- the risk is within acceptable limits;
- mitigation costs outweigh benefits;
- effective controls are already in place.

Accepted risks shall continue to be monitored.

5.4.5 Risk Exploitation

Where risks present potential opportunities, ILA may take deliberate action to maximize beneficial outcomes.

Examples include:

- strategic partnerships;
- innovative programme approaches;
- technology improvements;
- new funding opportunities.

5.5 Risk Treatment Plans

For all High and Critical risks, ILA shall develop a documented Risk Treatment Plan.

The Risk Treatment Plan shall include:

- description of the risk;
- existing controls;
- additional mitigation measures;
- responsible person;
- implementation timeline;
- required resources;
- monitoring indicators;
- expected outcomes.

5.6 Risk Owners and Accountability

Every significant risk shall have an assigned Risk Owner.

The Risk Owner shall:

- monitor the risk;
- implement agreed mitigation measures;
- report changes in risk exposure;
- maintain relevant documentation;
- ensure corrective actions are completed.

Assignment of risk ownership does not remove overall accountability from management.

5.7 Internal Control Framework

ILA shall maintain an effective internal control framework designed to provide reasonable assurance that organizational objectives are achieved.

Internal controls shall address:

- operational effectiveness;
- financial integrity;
- legal compliance;
- safeguarding;
- information security;

- asset protection;
- fraud prevention.

5.8 Types of Internal Controls

ILA shall apply the following categories of controls:

5.8.1 Preventive Controls

Preventive controls are designed to stop problems before they occur.

Examples include:

- approval procedures;
- segregation of duties;
- background checks;
- access restrictions;
- procurement procedures;
- authorization requirements.

5.8.2 Detective Controls

Detective controls identify problems after they occur.

Examples include:

- audits;
- reconciliations;
- monitoring reviews;
- inspections;
- complaints mechanisms;
- incident reporting.

5.8.3 Corrective Controls

Corrective controls address identified weaknesses and prevent recurrence.

Examples include:

- corrective action plans;
- disciplinary measures;
- system improvements;
- additional training.

5.9 Segregation of Duties

ILA shall maintain appropriate segregation of duties to reduce the risk of errors, fraud and abuse of authority.

Where practical, different individuals shall be responsible for:

- authorization;
- execution;
- recording;
- review;
- verification.

No individual shall control an entire transaction process without appropriate oversight.

5.10 Approval and Authorization Controls

ILA shall establish approval requirements for:

- financial transactions;
- procurement decisions;
- recruitment;
- contracts;
- asset disposal;
- programme changes;
- partnership agreements.

Approval limits shall be established through the Delegation of Authority framework.

5.11 Financial Risk Controls

Financial risks shall be managed through:

- approved budgets;
- financial reporting;
- expenditure authorization;
- bank reconciliation;
- cash controls;
- asset verification;
- audit processes;
- fraud prevention measures.

Financial risk management shall operate in accordance with the Finance and Accounting Policy.

5.12 Procurement Risk Controls

Procurement risks shall be managed through:

- procurement planning;
- competitive sourcing;
- supplier due diligence;
- conflict of interest declarations;
- procurement committees where applicable;
- contract management;
- supplier performance monitoring.

Procurement risk management shall comply with the Procurement and Asset Management Policy.

5.13 Fraud and Corruption Risk Controls

ILA has zero tolerance for fraud and corruption.

Fraud risks shall be managed through:

- ethical leadership;
- staff awareness;
- segregation of duties;
- financial controls;
- whistleblowing mechanisms;
- investigations;
- sanctions where misconduct is established.

Fraud-related risks shall be managed in accordance with the Anti-Fraud, Corruption and Whistleblowing Policy.

5.14 Safeguarding Risk Controls

Safeguarding risks shall be managed through:

- PSEAH procedures;
- staff screening;
- safeguarding training;
- reporting mechanisms;
- survivor-centred responses;
- accountability measures.

All safeguarding risks shall receive priority attention due to their potential impact on human dignity and safety.

5.15 Human Resource Risk Controls

HR risks shall be managed through:

- transparent recruitment;
- clear job descriptions;
- staff induction;
- performance management;
- staff development;
- disciplinary procedures;
- workplace safety measures.

5.16 ICT and Information Security Controls

ICT risks shall be controlled through:

- user access management;
- password protection;
- data backups;
- cybersecurity awareness;
- system monitoring;
- incident response procedures.

ICT controls shall align with the ICT Policy.

5.17 Legal and Compliance Controls

ILA shall manage compliance risks through:

- legal review;
- regulatory monitoring;
- contract management;
- policy compliance;
- timely reporting;
- record keeping.

5.18 Programme Risk Controls

Programme risks shall be managed through:

- sound programme design;
- logical frameworks;
- risk assessments;
- monitoring systems;
- beneficiary feedback;
- quality assurance mechanisms;

- lessons learned.

Programme risk management shall be integrated with the MEAL framework.

5.19 Security Risk Controls

Security risks shall be managed through:

- security assessments;
- staff awareness;
- travel procedures;
- emergency communication;
- incident response planning;
- contingency arrangements.

5.20 Risk Treatment Monitoring

Management shall monitor the effectiveness of risk treatment measures by assessing:

- whether actions were completed;
- whether controls are working;
- whether risk levels have changed;
- whether additional measures are required.

5.21 Corrective Action Management

Where weaknesses are identified, corrective actions shall be documented and tracked.

Corrective Action Plans shall specify:

- identified weakness;
- required action;
- responsible person;
- deadline;
- completion status;
- verification method.

5.22 Documentation Requirements

Risk treatment activities shall be documented through:

- Risk Registers;
- Risk Treatment Plans;
- Audit reports;
- Incident reports;
- Corrective Action Registers;

- Management review records.

5.23 Review of Risk Controls

Internal controls shall be reviewed periodically to ensure they remain:

- appropriate;
- effective;
- proportionate;
- aligned with organizational needs.

Reviews shall consider changes in:

- organizational structure;
- programmes;
- technology;
- legal requirements;
- operating environment.

CHAPTER SIX

SPECIALIZED RISK MANAGEMENT FRAMEWORK

6.1 Introduction

ILA recognizes that different categories of risks require specialized approaches, expertise and control measures. While the general risk management framework applies across the organization, certain risks require additional procedures due to their complexity, potential impact or regulatory significance.

This Chapter establishes specialized risk management requirements for key areas of organizational exposure.

The purpose of specialized risk management is to ensure that risks affecting ILA's mission, programmes, people, resources and reputation are managed through appropriate controls, ownership and monitoring mechanisms.

6.2 Strategic Risk Management

6.2.1 Overview

Strategic risks are risks that may affect ILA's ability to achieve its vision, mission, strategic objectives and long-term sustainability.

Strategic risks require continuous attention from leadership because they may have significant consequences for the organization's future direction.

6.2.2 Sources of Strategic Risks

Strategic risks may arise from:

- changes in the legal and regulatory environment;
- changes in government policy;
- political instability;
- funding uncertainty;
- changing donor priorities;
- failure to adapt to emerging needs;
- inadequate strategic planning;
- ineffective partnerships;
- loss of organizational legitimacy;
- inability to maintain institutional capacity.

6.2.3 Strategic Risk Controls

ILA shall manage strategic risks through:

- periodic strategic planning;
- environmental analysis;
- stakeholder engagement;
- organizational performance reviews;
- resource planning;
- leadership oversight;
- monitoring of strategic objectives.

6.2.4 Board Oversight

The Board of Directors shall periodically review strategic risks and ensure that management actions are aligned with the organization's mission and sustainability objectives.

6.3 Programme and Project Risk Management

6.3.1 Overview

Programme and project risks relate to factors that may prevent ILA from successfully delivering planned activities, achieving intended results or meeting donor obligations.

6.3.2 Programme Risk Identification

Programme teams shall identify risks relating to:

- programme design;
- implementation capacity;
- beneficiary access;

- stakeholder engagement;
- technical quality;
- monitoring and reporting;
- sustainability;
- donor compliance.

6.3.3 Programme Risk Controls

ILA shall manage programme risks through:

- programme risk assessments;
- logical frameworks;
- implementation plans;
- monitoring systems;
- beneficiary feedback mechanisms;
- quality assurance processes;
- regular programme reviews;
- lessons learned exercises.

6.3.4 Project Risk Registers

Every significant programme or project shall maintain a Project Risk Register containing:

- identified risks;
- risk ratings;
- mitigation measures;
- responsible officers;
- review dates.

6.4 Financial Risk Management

6.4.1 Overview

Financial risk management ensures that ILA's financial resources are protected, properly managed and used in accordance with approved purposes.

6.4.2 Financial Risk Areas

Financial risks include:

- fraud and corruption;
- inaccurate financial reporting;
- budget overruns;
- cash flow shortages;
- donor disallowances;
- unauthorized expenditure;

- taxation failures;
- poor financial controls;
- loss of assets.

6.4.3 Financial Risk Controls

ILA shall manage financial risks through:

- approved budgets;
- financial procedures;
- authorization controls;
- segregation of duties;
- bank reconciliation;
- expenditure verification;
- financial reporting;
- internal and external audits.

6.4.4 Donor Financial Compliance

All donor-funded activities shall be managed in accordance with:

- donor agreements;
- approved budgets;
- applicable financial rules;
- reporting requirements.

6.5 Fraud and Corruption Risk Management

6.5.1 Overview

Fraud and corruption present serious risks to ILA's resources, credibility and ability to achieve its mission.

ILA maintains zero tolerance for fraud, bribery, corruption, theft, abuse of authority and financial misconduct.

6.5.2 Fraud Risk Sources

Fraud risks may arise from:

- financial transactions;
- procurement processes;
- payroll;
- asset management;
- recruitment;
- conflicts of interest;

- misuse of organizational resources.

6.5.3 Fraud Risk Controls

ILA shall manage fraud risks through:

- ethical leadership;
- staff awareness;
- conflict of interest declarations;
- whistleblowing mechanisms;
- financial controls;
- investigations;
- disciplinary action;
- recovery of losses where applicable.

6.5.4 Relationship with Anti-Fraud Policy

Fraud risks shall be managed together with the Anti-Fraud, Corruption and Whistleblowing Policy, which provides detailed procedures for reporting, investigation and response.

6.6 Human Resource Risk Management

6.6.1 Overview

ILA recognizes that its personnel are central to achieving its objectives. Human resource risks may affect organizational effectiveness, culture, safety and sustainability.

6.6.2 HR Risk Areas

HR risks include:

- inability to recruit qualified personnel;
- high staff turnover;
- inadequate capacity;
- misconduct;
- workplace conflict;
- poor performance;
- inadequate succession planning;
- staff welfare concerns.

6.6.3 HR Risk Controls

ILA shall manage HR risks through:

- transparent recruitment;
- staff induction;

- performance management;
- professional development;
- succession planning;
- employee welfare programmes;
- disciplinary procedures.

6.7 Safeguarding Risk Management

6.7.1 Overview

ILA recognizes its duty to protect beneficiaries, staff and stakeholders from harm, exploitation, abuse and harassment.

Safeguarding risks require priority management because failures may result in serious harm to individuals and significant reputational consequences.

6.7.2 Safeguarding Risk Areas

These include:

- sexual exploitation and abuse;
- sexual harassment;
- abuse of vulnerable persons;
- misuse of authority;
- unsafe programme environments;
- failure to report concerns.

6.7.3 Safeguarding Controls

ILA shall manage safeguarding risks through:

- PSEAH Policy implementation;
- safeguarding training;
- staff screening;
- reporting channels;
- survivor-centred response;
- confidentiality measures;
- accountability procedures.

6.8 Security and Safety Risk Management

6.8.1 Overview

ILA operates in environments where security risks may affect personnel, beneficiaries, assets and programme delivery.

6.8.2 Security Risk Areas

Security risks may include:

- armed conflict;
- civil unrest;
- crime;
- threats against personnel;
- travel incidents;
- workplace hazards;
- health emergencies.

6.8.3 Security Controls

ILA shall manage security risks through:

- security assessments;
- staff briefings;
- emergency procedures;
- communication systems;
- incident reporting;
- contingency planning.

6.9 ICT and Cybersecurity Risk Management

6.9.1 Overview

Information and communication technology systems support ILA's operations and therefore require effective protection.

6.9.2 ICT Risk Areas

These include:

- unauthorized access;
- cyber-attacks;
- data loss;
- system failure;
- malware;
- privacy breaches;
- inadequate backups.

6.9.3 ICT Risk Controls

ILA shall manage ICT risks through:

- access controls;
- password management;
- data backups;
- cybersecurity awareness;
- system maintenance;
- incident response procedures.

6.10 Legal and Compliance Risk Management

6.10.1 Overview

ILA shall ensure that its activities comply with applicable laws, regulations, agreements and internal policies.

6.10.2 Compliance Risk Areas

These include:

- regulatory obligations;
- registration requirements;
- employment laws;
- taxation;
- contracts;
- donor conditions.

6.10.3 Compliance Controls

ILA shall manage compliance risks through:

- legal review;
- compliance monitoring;
- documentation;
- regulatory reporting;
- policy implementation.

6.11 Partnership and Third-Party Risk Management

6.11.1 Overview

Partnerships enable ILA to expand impact but may introduce risks relating to capacity, compliance and reputation.

6.11.2 Partnership Risk Areas

These include:

- inadequate partner capacity;
- misuse of funds;
- safeguarding failures;
- poor programme delivery;
- reputational damage.

6.11.3 Partnership Controls

ILA shall manage partner risks through:

- due diligence;
- partner assessments;
- written agreements;
- monitoring;
- reporting requirements;
- audits where necessary.

6.12 Reputational Risk Management

6.12.1 Overview

ILA's reputation is a valuable organizational asset. Loss of public trust may affect partnerships, funding and programme effectiveness.

6.12.2 Sources of Reputational Risk

These include:

- misconduct;
- poor programme performance;
- negative publicity;
- misuse of resources;
- failure to respond appropriately to incidents.

6.12.3 Reputational Risk Controls

ILA shall manage reputational risks through:

- ethical conduct;
- transparency;
- accountability;
- effective communication;

- stakeholder engagement;
- responsible public representation.

6.13 Environmental and Climate Risk Management

6.13.1 Overview

ILA recognizes that environmental and climate-related factors may affect organizational operations and programme delivery.

6.13.2 Environmental Risk Areas

These include:

- natural disasters;
- climate-related disruptions;
- environmental harm;
- resource limitations.

6.13.3 Environmental Risk Controls

ILA shall promote:

- environmentally responsible operations;
- sustainable practices;
- emergency preparedness;
- consideration of environmental impacts in programme design.

6.14 Integration of Specialized Risks

Specialized risks shall not be managed independently but shall be integrated into the overall Enterprise Risk Management framework.

Departments shall ensure that specialized risks are:

- identified;
- assessed;
- recorded;
- treated;
- monitored;
- reported.

6.15 Review of Specialized Risks

Specialized risks shall be reviewed:

- annually;
- during strategic planning;
- following major incidents;
- when operating environments change;
- when new programmes or partnerships are introduced.

CHAPTER SEVEN

RISK MONITORING, REPORTING, BUSINESS CONTINUITY AND CRISIS MANAGEMENT

7.1 Introduction

Risk management is an ongoing process that requires continuous monitoring, reporting, review and adaptation. Risks evolve as organizational activities, operating environments, legal requirements and stakeholder expectations change.

Initiative for Legal Aid (ILA) shall maintain effective mechanisms to ensure that risks are regularly monitored, accurately reported and appropriately managed. The organization shall also maintain preparedness arrangements to ensure continuity of critical operations during disruptions, emergencies and crises.

This Chapter establishes the requirements for:

- risk monitoring;
- risk reporting;
- incident escalation;
- Key Risk Indicators;
- business continuity planning;
- crisis management;
- lessons learned and organizational improvement.

7.2 Purpose of Risk Monitoring and Reporting

Risk monitoring and reporting aim to:

a) Ensure risks remain visible to appropriate decision-makers;

b) Identify changes in risk exposure;

c) Assess effectiveness of controls and mitigation measures;

d) Enable timely corrective action;

e) Support informed management and Board decisions;

f) Strengthen accountability and transparency;

g) Improve organizational resilience.

7.3 Risk Monitoring Framework

ILA shall establish a structured risk monitoring framework involving:

- continuous operational monitoring;
- departmental reviews;
- management reviews;
- Board oversight;
- audits and assessments;
- incident reviews;
- programme monitoring.

Risk monitoring shall be integrated into normal management processes and shall not be treated as a separate activity.

7.4 Continuous Risk Monitoring

All managers shall continuously monitor risks within their areas of responsibility.

Continuous monitoring shall include:

- changes in operating conditions;
- effectiveness of controls;
- emerging threats;
- implementation of mitigation actions;
- occurrence of incidents;
- changes in risk ratings.

Where significant changes occur, risks shall be reassessed and updated in relevant risk registers.

7.5 Risk Registers

7.5.1 Purpose of Risk Registers

Risk Registers are the primary tools for documenting and monitoring organizational risks.

ILA shall maintain:

- Organizational Risk Register;
- Departmental Risk Registers;
- Programme/Project Risk Registers;
- Incident Risk Register where applicable.

7.5.2 Minimum Information Required

Each Risk Register shall include:

- risk identification number;
- risk category;
- description of risk;
- causes and consequences;
- affected objectives;
- likelihood rating;
- impact rating;
- overall risk rating;
- existing controls;
- mitigation actions;
- risk owner;
- review date;
- status.

7.6 Key Risk Indicators (KRIs)

7.6.1 Purpose of KRIs

Key Risk Indicators are measurable indicators used to identify changes in risk exposure before significant problems occur.

7.6.2 Examples of KRIs

ILA may monitor indicators such as:

Financial KRIs

- budget variance;
- delayed financial reports;
- unresolved audit findings;
- cash flow challenges.

Human Resource KRIs

- staff turnover;
- vacancies in critical positions;
- unresolved grievances;
- training completion rates.

Programme KRIs

- delayed activities;

- low achievement of indicators;
- beneficiary complaints;
- implementation delays.

Safeguarding KRIs

- safeguarding reports;
- unresolved cases;
- training completion levels.

ICT KRIs

- security incidents;
- unauthorized access attempts;
- system downtime;
- backup failures.

7.7 Risk Reporting Structure

Risk reporting shall occur through the following channels:

7.7.1 Departmental Reporting

Department Heads shall report significant risks to Senior Management.

Reports shall include:

- current risk status;
- changes in exposure;
- mitigation progress;
- required decisions.

7.7.2 Management Risk Review

Senior Management shall periodically review:

- organizational risks;
- high and critical risks;
- mitigation progress;
- emerging risks.

Risk review shall form part of management meetings where appropriate.

7.7.3 Board Reporting

The Executive Director shall provide the Board with periodic risk reports.

Board reports shall include:

- major organizational risks;
- changes in risk exposure;
- critical incidents;
- mitigation actions;
- recommendations requiring Board attention.

7.8 Risk Escalation Framework

Risks shall be escalated based on their severity and potential consequences.

Immediate escalation shall be required where risks:

- threaten life or safety;
- involve fraud or corruption;
- involve safeguarding concerns;
- may cause significant financial loss;
- may seriously damage organizational reputation;
- may interrupt critical operations.

7.9 Incident Management

7.9.1 Definition of Incident

An incident is an event that has caused or may cause:

- harm;
- loss;
- disruption;
- legal exposure;
- reputational damage;
- failure of organizational objectives.

7.9.2 Incident Reporting

All personnel shall promptly report incidents through established reporting channels.

Examples include:

- fraud;
- safeguarding concerns;
- security incidents;
- data breaches;
- accidents;
- misuse of resources.

7.9.3 Incident Response

ILA shall respond to incidents through:

1. Immediate protection of people and assets;
2. Assessment of the situation;
3. Notification of responsible persons;
4. Investigation where required;
5. Corrective action;
6. Documentation;
7. Lessons learned.

7.10 Business Continuity Management

7.10.1 Purpose

Business continuity management ensures that ILA can continue essential operations during and after major disruptions.

7.10.2 Business Continuity Principles

ILA shall ensure:

- protection of personnel;
- preservation of critical information;
- continuity of essential programmes;
- timely recovery of operations;
- effective communication during emergencies.

7.11 Business Continuity Planning

ILA shall maintain a Business Continuity Plan addressing:

- critical organizational functions;
- potential disruptions;
- emergency responsibilities;
- communication arrangements;
- alternative working arrangements;
- recovery priorities;
- resource requirements.

7.12 Critical Functions

Critical functions may include:

- safeguarding systems;

- financial operations;
- essential programme activities;
- communication systems;
- legal and regulatory obligations;
- protection of organizational records.

7.13 Business Continuity Response Levels

ILA may activate different response levels depending on the severity of disruption.

Level One: Minor Disruption

Examples:

- temporary system failure;
- localized operational challenge.

Response:

- departmental management action;
- normal recovery procedures.

Level Two: Significant Disruption

Examples:

- extended operational interruption;
- serious security concern.

Response:

- management coordination;
- activation of contingency arrangements.

Level Three: Major Crisis

Examples:

- major security incident;
- severe reputational event;
- disaster affecting operations.

Response:

- activation of Crisis Management Team;

- Board notification;
- full emergency response.

7.14 Crisis Management Framework

7.14.1 Crisis Definition

A crisis is a serious event that threatens:

- organizational survival;
- personnel safety;
- beneficiaries;
- reputation;
- critical operations.

7.14.2 Crisis Management Team

ILA may establish a Crisis Management Team consisting of:

- Executive Director;
- Senior Management representatives;
- Security focal person;
- Finance representative;
- HR representative;
- Communications representative;
- Other relevant persons.

7.14.3 Crisis Management Responsibilities

The Crisis Management Team shall:

- assess the crisis;
- coordinate response;
- protect people and assets;
- manage communications;
- ensure continuity of operations;
- document decisions.

7.15 Emergency Communication

During emergencies, communication shall be:

- timely;
- accurate;
- coordinated;
- confidential where required.

Only authorized persons shall communicate externally on behalf of ILA during major incidents.

7.16 Recovery and Restoration

Following a crisis, ILA shall:

- restore critical operations;
- assess damages;
- support affected personnel;
- address outstanding risks;
- review response effectiveness.

7.17 Lessons Learned

After significant incidents or crises, ILA shall conduct reviews to determine:

- what happened;
- causes of the event;
- effectiveness of response;
- improvements required.

Lessons learned shall inform future risk management practices.

7.18 Audits and Independent Reviews

Where appropriate, ILA may conduct:

- internal reviews;
- external audits;
- donor assessments;
- independent evaluations.

Findings shall be documented and corrective actions monitored.

7.19 Risk Management Performance Review

Management shall periodically assess whether the risk management framework remains:

- effective;
- appropriate;
- adequately resourced;
- aligned with organizational objectives.

7.20 Continuous Improvement

ILA shall continuously strengthen its risk management approach through:

- training;
- policy updates;
- improved systems;
- adoption of lessons learned;
- stakeholder feedback.

CHAPTER EIGHT

POLICY IMPLEMENTATION, TRAINING, COMPLIANCE, REVIEW AND AMENDMENT

8.1 Introduction

The effectiveness of this Risk Management Policy depends on its proper implementation, continuous awareness, institutional ownership and consistent application throughout Initiative for Legal Aid (ILA).

ILA recognizes that a policy document alone does not create effective risk management. Effective implementation requires leadership commitment, adequate resources, staff capacity, accountability mechanisms and continuous monitoring.

This Chapter establishes the arrangements for implementing, communicating, monitoring compliance with, reviewing and updating this Policy.

8.2 Policy Implementation Framework

ILA shall implement this Policy through a coordinated approach involving:

- Board oversight;
- executive leadership;
- management accountability;
- departmental implementation;
- staff awareness;
- operational procedures;
- monitoring and review mechanisms.

Implementation shall ensure that risk management becomes part of ILA's organizational culture and routine decision-making processes.

8.3 Responsibilities for Policy Implementation

8.3.1 Board of Directors

The Board shall:

- approve this Policy;

- provide governance oversight;
- review significant risk matters;
- ensure management accountability;
- approve major amendments.

8.3.2 Executive Director

The Executive Director shall:

- lead implementation of this Policy;
- ensure adequate resources are available;
- promote risk awareness;
- ensure compliance across the organization;
- report significant risks to the Board.

8.3.3 Senior Management

Senior Management shall:

- translate this Policy into operational practice;
- ensure departmental compliance;
- review organizational risk exposure;
- monitor implementation progress;
- support continuous improvement.

8.3.4 Department Heads

Department Heads shall:

- implement risk management measures within their departments;
- maintain relevant risk registers;
- ensure staff compliance;
- report emerging risks;
- implement corrective actions.

8.3.5 All Personnel

All personnel shall:

- understand their risk responsibilities;
- comply with this Policy;
- participate in risk management activities;
- report risks and incidents;
- protect organizational resources.

8.4 Risk Management Training and Capacity Building

8.4.1 Commitment to Training

ILA shall provide appropriate training to ensure that personnel have the knowledge and skills necessary to identify, assess and manage risks effectively.

8.4.2 Training Objectives

Risk management training shall aim to:

- promote awareness of organizational risks;
- strengthen risk identification skills;
- improve understanding of internal controls;
- promote ethical decision-making;
- strengthen incident reporting;
- improve compliance with organizational policies.

8.4.3 Target Groups

Training shall be provided to:

- Board members;
- managers;
- programme staff;
- finance staff;
- procurement staff;
- ICT personnel;
- HR personnel;
- new employees;
- volunteers and interns where relevant.

8.4.4 Training Methods

Training may include:

- induction sessions;
- workshops;
- refresher training;
- online learning;
- management briefings;
- policy awareness sessions.

8.5 Staff Induction

All new personnel shall receive appropriate orientation on:

- ILA's risk management approach;

- their responsibilities under this Policy;
- incident reporting procedures;
- relevant organizational policies;
- ethical obligations.

Risk management awareness shall form part of staff onboarding processes.

8.6 Communication and Awareness

ILA shall ensure that this Policy is communicated effectively through:

- staff meetings;
- internal communications;
- training sessions;
- organizational platforms;
- policy dissemination processes.

Personnel shall have access to the current approved version of this Policy.

8.7 Compliance Monitoring

ILA shall monitor compliance with this Policy through:

- management reviews;
- internal audits;
- external audits;
- donor assessments;
- programme reviews;
- compliance checks;
- incident reviews.

8.8 Risk Management Assurance

ILA may undertake assurance activities to determine whether:

- risks are appropriately identified;
- controls are functioning effectively;
- mitigation actions are implemented;
- reporting systems are reliable.

Assurance activities may be conducted by:

- internal reviewers;
- external auditors;
- consultants;
- donor representatives;

- independent assessors.

8.9 Non-Compliance with the Policy

Failure to comply with this Policy may expose ILA to legal, financial, operational and reputational risks.

Where non-compliance is identified, ILA may take appropriate action including:

- corrective measures;
- additional training;
- management intervention;
- performance management;
- disciplinary action;
- contractual remedies;
- reporting to relevant authorities where required.

Actions shall be undertaken in accordance with:

- the Human Resource and Administration Manual;
- employment contracts;
- applicable laws;
- principles of fairness and due process.

8.10 Documentation and Record Keeping

ILA shall maintain appropriate records relating to risk management, including:

- risk assessments;
- risk registers;
- mitigation plans;
- incident reports;
- investigation reports;
- audit findings;
- corrective actions;
- training records;
- review reports.

Records shall be maintained in accordance with the ICT Policy and Records Management requirements.

8.11 Confidentiality and Information Protection

Risk-related information may contain sensitive organizational, financial, security or personal information.

ILA shall ensure that:

- confidential information is protected;
- access is limited to authorized persons;
- information is shared only on a need-to-know basis;
- personal information is handled appropriately.

Confidentiality obligations shall not prevent reporting of serious risks, misconduct or unlawful conduct.

8.12 Relationship with Other Policies

This Policy shall operate together with other ILA policies.

Where specialized procedures exist under another policy, those procedures shall apply while remaining consistent with this Risk Management Policy.

Key related policies include:

- Finance and Accounting Policy;
- Procurement and Asset Management Policy;
- ICT Policy;
- Human Resource and Administration Manual;
- MEAL Policy;
- PSEAH Policy;
- Anti-Fraud, Corruption and Whistleblowing Policy;
- Code of Conduct and Ethics Policy.

8.13 Policy Review

This Policy shall be reviewed periodically to ensure continued relevance and effectiveness.

The review shall consider:

- organizational changes;
- changes in legal requirements;
- donor expectations;
- lessons learned;
- audit recommendations;
- emerging risks;
- operational experience.

8.14 Review Frequency

The Policy shall be reviewed at least once every:

Three (3) years

or earlier where circumstances require.

8.15 Policy Amendment Process

Amendments to this Policy may be proposed by:

- the Board;
- Executive Director;
- Senior Management;
- relevant committees;
- policy review teams.

Proposed amendments shall:

1. Be documented;
2. Be reviewed for consistency;
3. Be approved through appropriate governance procedures;
4. Be communicated to all relevant personnel.

8.16 Version Control

ILA shall maintain proper version control for this Policy, including:

- policy version number;
- approval date;
- effective date;
- review date;
- amendment history;
- approving authority.

8.17 Effective Date

This Policy shall become effective on the date approved by the Board of Directors of Initiative for Legal Aid.

8.18 Approval

Approved by:

Board of Directors
Initiative for Legal Aid (ILA)

Board Resolution No.: _____

Approval Date: _____

Effective Date: _____

Policy Owner: Executive Director

Next Review Date: _____

8.19 Conclusion

Effective risk management is essential to the sustainability, accountability and success of Initiative for Legal Aid.

Through this Policy, ILA commits to maintaining a proactive, integrated and accountable approach to managing uncertainty, protecting stakeholders and achieving its mission.

Risk management shall remain a shared responsibility supported by ethical leadership, effective systems, continuous learning and organizational commitment.