Risk Management Policy

Libyan Investment Authority

Contents

1. Introduction

The set of guidelines contained in this document form the basis of the Risk Management Policy of the Libyan Investment Authority ("LIA").

1.1. Applicability and scope

This document sets out the high-level principles, controls and frameworks for the LIA's management of its key risks. The document is structured to outline the LIA's risk-taking in the context of its strategic objectives as well as its tolerance and capacity for risk-taking.

The main risks are divided into two broad categories: Investment Risk and Enterprise Risk. Each category is then sub-divided into risk types. Definitions and sources for each risk type are identified, and risk management principles are outlined, including risk monitoring. The risk management principles outlined here are implemented through operational guidelines, limits, and methodologies and tools for measuring, monitoring and reporting risk.

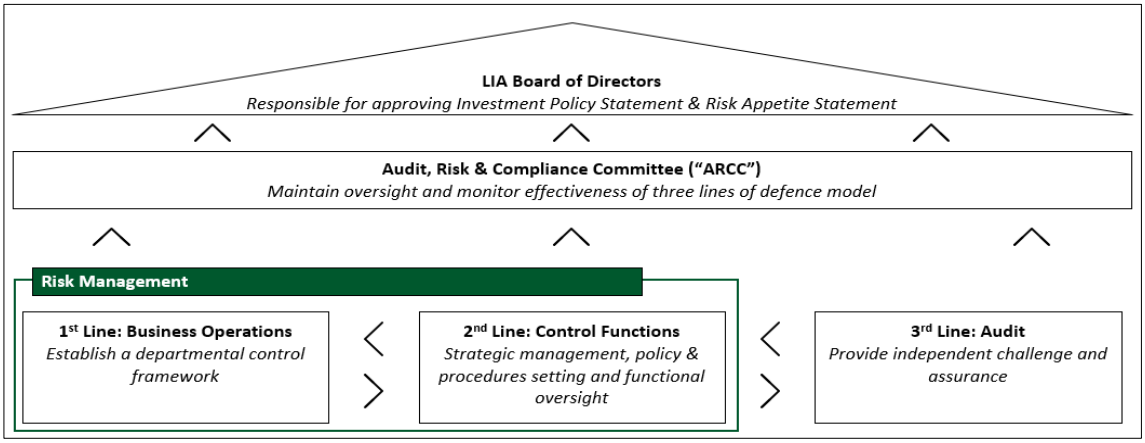
1.2. General principles

The LIA is entrusted to protect and grow the wealth of the Libyan people for future generations. In order to do this, the LIA must ensure it manages risk in a proactive and measured manner, noting that risk is an integral part of investment. Risk is characterised by uncertainty and is measured in terms of the potential impact of an occurrence and the likelihood of the event taking place.

The LIA is committed to a strategy that supports the identification, measurement, monitoring and reporting of key risks, and uses the information assembled through this process to enhance its decision-making. The LIA shall adopt the widely accepted 'three lines of defence' model, which establishes the broader framework for risk management, as shown in

Figure 1 below.

Figure 1: LIA Risk Management Framework



Risk Management responsibilities will be divided between business operations and control functions at the LIA, while Audit will provide independent challenge and assurance. The specific amount and types of risk the LIA is willing to take in order to meet its strategic objectives will be defined under a separate Risk Appetite Statement ("RAS").

1.3. Risk Appetite Statement

Risk Appetite is an upper bound limit of risk that should be taken articulated in terms of a fund's net asset value, liquidity or similar metric. The LIA's Risk Appetite Statement will be developed iteratively, through discussions with the LIA's management team, Risk Department, and Board of Directors on the form and level of the risk that the LIA is willing to take during the stages of the organisation's structural development. The RAS will:

- Outline the specific amount and types of risk the LIA is willing to take across each risk type in order to meet its strategic objectives;
- Define risk types and the LIA's potential exposure to each;
- Articulate the rationale developed by the LIA to determine the appropriate risk appetites for each risk type;
- Outline the approach used to identify, measure, manage, monitor and report on actual exposures the LIA has to each risk type in comparison to the initial risk appetites determined by the LIA;
- Define the mitigating approach to take in the event of any breaches to the risk appetite; and
- Outline the qualitative statements used to define the behaviour and risk culture of the LIA.

As the definitions, processes and risk limits are identified in the RAS, this Policy document will provide guidance on the monitoring and management of each risk type.

1.4. Risk level identification

The LIA's risk management function shall monitor the overall risk exposure and shall compare the risk exposure to the RAS and the LIA's overall risk tolerance. Identified risks, risk levels and exposure shall be reviewed on a regular basis and incidents followed up by each risk owner to ensure necessary investigation and escalation where necessary. The LIA shall ensure that suitable processes are in place in order to ensure prompt and accurate risk monitoring.

The LIA defines the risk level as a combination of the probability / frequency of an event's occurrence and the potential consequence should the event occur, across all risk types. The LIA defines four risk levels in order to determine mitigation strategies: Critical, Significant, Moderate and Insignificant. Risk level exposures are regularly communicated to senior management, as well as the Audit, Risk and Compliance Committee ("ARCC") of the Board of Directors ("BoD"). If risk exposures exceed the limits set for individual assets or for the portfolios, rebalancing is required. Individual investments that exceed established risk limits must be approved by the Board.

Risks identified as:

- Critical risks are deemed unacceptable for the LIA, and therefore immediate mitigating actions must be taken. Only the Board of Directors may accept Critical risks without taking further mitigating actions. In such cases the ARCC must be kept informed of all developments.
- Significant are also deemed unacceptable for the LIA, and as such risk mitigating actions shall be initiated and followed up promptly. Only the Chief Executive Officer ("CEO") may accept Significant risks without additional risk mitigation. In such cases the BoD and the ARCC must be kept informed of all developments.
- Moderate are deemed acceptable for the LIA, but risk mitigating actions will be considered on a case-by-case basis.
- Insignificant are deemed acceptable for the LIA, but risk mitigating actions will be considered in order to improve the effectiveness of daily operations.

1.5. Risk culture

The LIA's risk management approach is underpinned and supported by the continued emphasis on risk awareness throughout the organisation. The LIA is committed to providing widespread training for its employees regarding risk management, and employees are expected to comply with the highest standards of integrity, competence, and professional ethics.

The LIA's risk culture shall be based around maximising ability to deliver the LIA's objectives, promoting sound decision-making, supporting the safeguarding of the LIA and its employees, and meeting the LIA's strategic objectives.

2. Investment Risk

Investment risk is defined as the risk of events affecting the performance of the LIA's assets and portfolios, and includes market risk, liquidity risk, credit risk and counterparty risk. The LIA aims to ensure that its combined assets are managed within the limits set out by the BoD and allocated to its investment strategies as set out by the investment policy. The LIA's Investment Directorate shall assess investment risk, providing the necessary flexibility to capture risks that are specific to each asset or asset class.

Investment risk is actively desired as in order to generate appropriate levels of return, the LIA needs to take risk. The objective is to ensure that the investment risk is commensurate or optimised versus the level of return targeted. This requires a suitably diversified portfolio across asset classes and investment styles. In the long term, the LIA's investment styles and therefore the investment risk it tolerates, may vary according to the LIA's investment objectives

The Risk Department will therefore monitor the adherence to the Strategic Asset Allocation (SAA) set and of concentration risks. It will also monitor where too little risk is being taken, and therefore the probability of achieving the targeted returns is at risk. The Risk Department will ensure that all portfolios have appropriate benchmarks and monitoring the tracking errors.

2.1. Market risk

Market risk is defined as the risk of the fund's market value fluctuating due to the volatility of financial market variables. Market risk can manifest through for example volatility / correlation risk – the economic risk to the LIA or its assets, driven often by systematic risk factors that apply to broader groups of assets (e.g. the impact of interest rates, macroeconomic shocks, foreign exchange rates).

The LIA takes market risk exposure each time it invests in an asset, the value of which can decline due to volatility in the market.

Value at Risk ("VaR") is an estimate of how much a set of investments might lose, given normal market conditions, in a set time period such as a day, month or year. The LIA will use VaR as one of the tools to determine the extent of potential asset / portfolio losses under a certain probability (expressed through a confidence interval) as compared to Risk Appetite limits. The LIA will use VaR to evaluate its market risk, including when analysing potential investments. In general, VaR can be calculated at both the individual asset level and at the portfolio level.

2.1.1. Management

The LIA should accept market risk to the extent that it is in line with the LIA's Investment Policy Statement ("IPS") and RAS. Considering this objective, the LIA should also ensure market risk events do not lead to the disruption of its investment operations. Market risks should also be considered and evaluated during the investment decision making process and considered appropriately before proceeding with any such decision.

The LIA aims to ensure exposure to market risk is in line with its approved RAS, including in an adverse event. Limits for market risk bearing capacity are to be defined in the RAS, and the LIA should have clear plans in place if positions or experienced losses exceed these limits to minimise damage from market risk events.

The LIA is not subject to specific regulation with regards to market risk management, and therefore the ultimate governing document in the area of market risk management is the RAS. In case of any conflicts between this policy and the RAS, the latter takes priority.

2.1.2. Monitoring

Market risk shall be monitored and assessed across both indictors of concentration risk and volatility / correlation risk. The LIA shall aim to ensure that all its assets and portfolios are appropriately structured and given due consideration under the ongoing risk assessment and monitoring. Regular stress testing to model potential performance and losses under extraordinary market conditions shall be conducted and included in monthly reporting. For volatility / correlation risk, the LIA shall monitor the standard deviation of expected returns on its investments.

The LIA should aim to ensure a high level of transparency surrounding its market risk exposure for Executive Management, the ARCC, and the BoD via monthly reporting.

2.2. Credit risk

Credit risk is defined as the risk of losses related to an issuer or borrower defaulting or being unable to meet their obligations. The risk is that of the lender and includes lost principal and interest, disruption to cash flows, and increased collection costs.

If an issuer or borrower has not made a scheduled payment of interest or principal within 30 business days of the scheduled payment, or a bond covenant is breached, the issuer (or borrower) has defaulted. If an assessment concludes it unlikely that the issuer or borrower will pay its obligations in full, the LIA may also deem that security as in default. Credit risk can derive from institutional or country-specific factors, as well as from credit migration events.

The LIA has significant cash balances at banks, and has made loans to other government institutions, and as such the Risk Department will actively manage the credit risks associated with these counterparties.

2.2.1. Management

The LIA should accept credit risk to the extent it is in line with the LIA's IPS and RAS. The LIA should aim to ensure credit risk events do not lead to the disruption of its business. The LIA should have clear plans and procedures in place if positions or experienced losses exceed credit risk limits to minimise the damage to the LIA from credit risk events.

The LIA shall follow set procedures for the management of default with the aim of achieving the highest possible recovery of its assets. The Head of Risk is responsible for informing the Director of Risk & Compliance and the ARCC in such instances to seek advice for further action. The LIA is not subject to specific regulation with regards to credit risk management, and therefore the ultimate governing document in the area of credit risk management is the RAS. In case of any conflicts between this policy and the RAS, the latter takes priority.

2.2.2. Monitoring

Credit risk shall be monitored continuously at both counterparty level and at portfolio level. The LIA shall include in its monthly reporting a credit exposure overview with respect to all investment instruments under the funds it manages and define criteria for the identification and monitoring of high-risk issuers or borrowers. The LIA shall also monitor the credit rating distribution for all issuers of fixed income instruments and define criteria for their assessment where credit ratings are not available.

The LIA should aim to ensure a high level of transparency with its credit risk exposures for Executive Management, the ARCC, and the BoD via monthly reporting. Credit risk should be considered and evaluated within the investment decision making process and considered appropriately before proceeding with any such decision.

2.3. Counterparty risk

Counterparty risk is defined as the risk of financial loss if a counterparty to a specific transaction defaults before the final settlement. It can arise through a variety of transactions (e.g. security trades, deposits, or security financing transactions), and could occur during settlement or via a custodian or sub-custodian bank. These risks could result in the failure of a counterparty to make payments by a deadline, deliver securities on time or of a vendor to deliver on a contract.

2.3.1. Selection and approval of counterparties

The LIA gets exposure to counterparty risk every time it:

- Acquires fixed income assets
- Lends funds to another entity
- Deposits funds with banks
- Enters derivative transaction for privately negotiated contracts (over the counter)
- Enters securities lending transactions
- Enters reverse repurchase agreement transactions

The LIA shall ensure that the requestor and approver of new counterparties are separated, and that the use of counterparties rests on a sound legal framework. The risk management function is responsible for approval of counterparties. The LIA shall select and use counterparties with the goal of reducing execution costs over time and mitigating concentration risk by ensuring the use of multiple counterparties.

Furthermore, the Risk Department shall ensure written agreements have been concluded when entering into a transaction and that the appropriate collateral is in place for any lending activity (e.g. collateral for the securities lending).

A counterparty list shall be maintained by the LIA's Risk Department, listing all approved counterparties.

2.3.2. Management

The LIA should accept counterparty risk to the extent that it is in line with the LIA's IPS and RAS and provides the LIA with an adequate risk premium for assuming it. The LIA should ensure counterparty risk events do not lead to the disruption of its business operations. The LIA should have clear plans in place if positions or experienced losses exceed counterparty risk limits to minimise the damage resulting in these risk events.

The LIA's risk department shall implement the needed controls and collateral to mitigate counterparty risk. This includes setting minimum collateral requirements and recording all re-investment of collateral in the established systems for risk measurement and compliance monitoring. Limits for counterparty risk shall be set within the service level agreements or investment management agreements signed with counterparties.

Counterparty risk should be considered and evaluated within the investment decision making process and considered appropriately before proceeding with any such decision. Procedures shall also be designed and implemented in order to manage the default and recovery of the LIA's assets in the event of counterparty default. The Head of Risk is responsible for informing

the Director of Risk & Compliance and the ARCC in such instances to seek advice for further action. The LIA is not subject to specific regulation with regards to counterparty risk management, and therefore the ultimate governing document in the area of counterparty risk management is the RAS. In case of any conflicts between this policy and the RAS, the latter takes priority.

2.3.3. Monitoring

The LIA's risk management function shall identify, assess and monitor counterparty risk across the LIA's portfolio, including monitoring minimum collateral requirements. Limits for counterparty risk shall be set via guidelines or investment mandates. The LIA should aim to ensure a high level of transparency surrounding its counterparty risk exposure to the Executive Management, the ARCC, and the BoD via monthly reporting.

2.4. Liquidity risk

Liquidity risk is the risk that a willing buyer might not be found when an asset needs to be sold, or that the LIA is not able to meet its obligations as they fall due.

In its business activities the LIA is required to always be able to meet its cash obligations for both external purposes (e.g. settlement obligations on financial instruments, payments to suppliers or vendors). The LIA also requires sufficient liquidity to carry out any strategic initiatives and cover any large or unexpected cash outflows. The LIA must therefore maintain sufficiently liquid assets within its investment portfolio, and recognise which of its assets are long-term and illiquid and therefore unable to contribute to the organisation's liquidity.

2.4.1. Management

The LIA should accept liquidity risk to the extent it is in line with the LIA's IPS and RAS. Under normal conditions, the LIA should manage its assets such that it is able to meet its liquidity needs for at least 90 days using cash or equivalent low-risk assets (e.g. money market investment funds that can be liquidated overnight, without seeking external funding sources).

The LIA will work to ensure liquidity risk events do not lead to the disruption of its business. The LIA should have clear plans in place if positions or the cash flow profile exceed liquidity risk limits to minimise the damage to the LIA from liquidity risk events.

The LIA is not subject to specific regulation with regards to liquidity risk management, and therefore the ultimate governing document in the area of liquidity risk management is the RAS. In case of any conflicts between this policy and the RAS, the latter takes priority.

2.4.2. Monitoring

The LIA should aim to ensure a high level of transparency with its liquidity reports and on its liquidity risk exposure for Executive Management, the ARCC, and the BoD via monthly reporting. Liquidity risks should also be considered within the investment decision making process and considered appropriately before proceeding with any such decision.

3. Enterprise Risk

Enterprise risk is defined as all risks affecting the LIA's organisation, operations and business. This includes the people, processes and day-to-day operations the organisation uses to manage risk as well as its strategy.

Reputational risk to the LIA is considered to be a potential consequence across all enterprise risk types and thus the management of reputational risk falls across these guidelines.

3.1. Operational risk

Operational risk stems from internal processes, people or systems failing to function, or from external factors or unwanted events causing financial or reputational loss to the LIA. Operational risk can lead to significant disruption to the LIA's business activities and cause material losses to the LIA. Examples include:

- Compliance risk: a failure to comply with laws, regulations, internal rules and codes of conduct applicable to the LIA's activities
- Strategic risk: the risk that the LIA or its leadership take inappropriate decisions or are unable to successfully implement the LIA's strategy
- Fraud risk: a deliberate deceptive act by an individual aimed at achieving an unjust or illegal advantage, committed by an internal (e.g. staff or contractors) or external party (e.g. External Fund Managers)

Operational risk could also impact the physical and IT infrastructure of the LIA, as well as the core business functions of the organisation.

For this reason, the monitoring and mitigation of operational risk shall be included in Business Continuity planning activities as detailed in Section 3.3.

3.1.1. Management

The LIA should accept operational risk to the extent it is in line with the LIA's RAS. The LIA should ensure that operational risk events do not lead to the disruption of its business

operations and have clear plans in place if losses or incidents exceed operational risk limits to minimise damage from operational risk events.

The LIA shall mitigate operational risk through:

- Systematically identifying and assessing risks across the organisation;
- Ensuring all employees report operational risks and incidents they encounter or suspect;
- Implementing effective mitigating measures and controls to reduce loss;
- Maintaining a key person risk framework to identify cover required for key roles in the event of staff absence; and
- Conducting internal audit reviews.

To mitigate against strategic risk, the LIA shall work to ensure that its strategic planning process minimises the adverse impact of undesirable events or adverse changes in the wider business environment. The strategy shall support the LIA's mission to protect and grow the wealth of the Libyan people for future generations.

Internal fraud risk shall be mitigated partially through a robust recruitment and selection process, ensuring LIA employees are people who adhere to strong ethical and professional standing. To mitigate against both internal and external fraud risk, the LIA shall ensure the effective application and enforcement of its policies, procedures and controls, including the Employee Code of Conduct and its Compliance Policy.

To mitigate against external fraud risk in particular the LIA will always conduct operational due diligence on potential third-party managers or external contractors.

The LIA is not subject to specific regulation with regards to operational risk management, and therefore the ultimate governing document in the area of operational risk management is the RAS. In case of any conflicts between this policy and the RAS, the latter takes priority.

3.1.2. Monitoring

Operational risk shall be monitored and assessed across compliance risk, strategic risk and fraud risk. Each shall be monitored through regular, systematic risk assessments and direct reports of operational risks or incidents by employees. The Head of Compliance shall support in monitoring and minimising compliance risk in all the LIA's operational, institutional and investment activities. The LIA should aim to ensure a high level of transparency surrounding its operational risk exposure for executive management, the ARCC, and the BoD via quarterly reporting.

3.2. Information security risk

Information security risk comprises the impact to the LIA of potential threats and vulnerabilities associated with its information systems and the environments in which they operate. Information security risk can lead to significant disruptions to the LIA's business activities and cause material losses to the LIA, as well as having significant legal and reputational impact.

3.2.1. Management

The LIA should accept information security risk to the extent it is in line with the LIA's RAS and cannot be mitigated at an appropriate cost. Information security risks shall be identified, assessed and mitigated according to the LIA's broader risk management framework.

The LIA aims to secure its information and its systems by ensuring appropriate standards are met in establishing and maintaining its systems and processes. Security expectations, processes and procedures are communicated to the LIA's employees through a set of policies and standards maintained throughout the organisation.

The LIA is not subject to specific regulation with regards to information security risk management, and therefore the ultimate governing document in the area of information security risk management is the RAS. In case of any conflicts between this policy and the RAS, the latter takes priority.

3.2.2. Monitoring

The LIA will monitor information systems, whether internally developed or externally sourced, to ensure that they are secure. It will also aim to ensure there is an appropriate incident response plan and solution in place should an incident threaten or damage its systems. The LIA should aim to ensure a high level of transparency surrounding its information security risk exposure for Executive Management, the ARCC, and the BoD via quarterly reporting.

3.3. Business continuity plan

Business continuity is the capability of an organisation to continue its operations at acceptable predefined levels following a disruptive incident with a low probability / frequency of occurrence but a high potential impact on the organisation's progress. A Business Continuity Plan ("BCP") aims to allow an organisation to effectively mitigate, minimise and manage the potential consequences of such situations should they occur, quickly enabling a recovery to normal or near-normal operation.

In its BCP activities, the LIA aims to protect:

- The welfare and security of its employees at all times;
- Its assets, resources and infrastructure, including those required to operate critical business processes; and
- Its reputation both within Libya and internationally.

The BCP shall include measures to:

- Clearly define key roles and responsibilities;
- Quickly re-establish key processes and activities whether locally in Libya or at one of its international recovery sites;
- Ensure the security of the LIA's employees, assets and resources;
- Ensure critical business functions can continue effectively including information systems and resources; and
- Enable detailed and effective crisis communication and media handling.

The Head of Risk alongside the Directors of Risk & Compliance and Director of Operations are responsible for the production and regular review of the BCP and for ensuring the broader resilience of the organisation. The ARCC shall ensure the implementation of the Business Continuity Plan, review it at least once every year, and raise related matters with Executive Management and the Board of Directors as appropriate.

4. Reporting

4.1. Regular reporting

The risk management function shall produce timely, accurate and consistent reports covering each risk type outlined in this document. The Head of Risk must produce reports to the BoD and ARCC on the following topics on a quarterly basis, and to the CEO on a monthly basis:

- The LIA's performance against risk limits;
- The status of monitoring and assessment activities including risk levels;
- Mitigation activities underway and planned;
- Assessment of reputational impact; and
- Incidents of fraud, operational risk and ongoing investigations.

The BoD, the ARCC and the CEO may recommend actions in order to mitigate key risks in line with the Risk Management Framework.

Annually, the Head of Risk shall prepare a statement outlining the LIA's overall status of risk, including reference to each dimension of risk outlined in this document and the risk levels applied to each.

In addition to regular standardised reporting, proactive risk analysis shall be performed and reported to the LIA's Executive Management team. The LIA's Internal Audit Department shall also be given access to risk material and regular reporting where required to form an assessment as the third line of defence.

4.2. Incident reporting

When incidents occur, the priority of the Risk Department and the employees involved in the incident is to resolve the incident and return to normal operations, regardless of the severity of the incident. Critical and significant operational incidents shall be reported to the BoD in any event. Where an incident could cause severe disruption to the LIA's core processes, the Business Continuity Plan shall be considered for activation by the BoD upon the advice of the ARCC.

All employees at the LIA shall be encouraged to engage in incident reporting, and no employees shall receive negative feedback or attention for doing so. Incidents of a sensitive nature that may impact on specific individuals (e.g. fraud, whistleblowing) will be treated and reported with care.

5. Review of Policy

The Head of Risk shall submit the Risk Management Policy to the Risk & Compliance Director for review and who shall subsequently obtain the approval of the CEO. The CEO shall then present the policy to the ARCC, and the ARCC will forward the request on to the BoD along with their recommendation.

The ARCC defines and monitors the adequacy and effectiveness of the LIA's risk management framework, policies and practices on an annual basis. The contents of the Policy shall be studied and reviewed at least every two years or as needed to account for changes in international standards, Libyan Law or the LIA's policies.

The Head of Risk is the custodian of this Policy and is expected to ensure that this document is an accurate representation of the applicable policies, and that it is kept up to date at all times.

If any dispute arises over the interpretation or application of this document, the Legal Affairs Directorate shall be responsible for interpreting the relevant laws and regulations. In the case of any unclear or ambiguous wording in the Arabic version of the Policy, the English version shall prevail.

6. Appendices

6.1. Appendix A: Definitions

In this document, the following definitions apply unless the context clearly requires otherwise:

- "Board" or "Board of Directors" refers to the Board of Directors of the Libyan Investment Authority.
- "CEO" or "Chief Executive Officer" refers to the Chief Executive Officer of the Libyan Investment Authority.
- "Counterparty" refers to an entity or group of entities with whom the LIA enters into business transactions
- "Employee" means any person working for the LIA and includes full time, part time, probationary, contract/temporary staff at the LIA.
- "LIA" or "the LIA" refer to the Libyan Investment Authority.
- "Risk" is any internal or external factor which poses a potential threat to the LIA's capacity to follow its strategy and achieve its objectives.
- "Subsidiary" or "the LIA's subsidiaries" include LTP, LAP, LAFICO, LLIDF and Oilinvest.
- "RAS" refers to Risk Appetite Statement
- "VAR" refers to the value at risk.