



Compliance Policy

Libyan Investment Authority

V1.0 March 2020

Document Owner: Head of Compliance Department

Name: _____ Signed: _____ Date: __/__/____

Document Approved by: Board of Directors

Name: _____ Signed: _____ Date: __/__/____

Document History:

| <i>Version</i> | <i>Date</i> | <i>Changes/Modifications</i> | <i>Approved by:</i> |
|----------------|-----------------|------------------------------|---------------------|
| 1.0 | .../.../2020 AD | - | |
| | | | |
| | | | |
| | | | |

Document to be next reviewed / updated by: Audit, Risk & Compliance Committee

Name: _____ Date of next review: __/__/____

Signed: _____



Contents

| | | |
|-----------|--|-----------|
| 1. | Introduction | 1 |
| 1.1. | Nature and Objectives of Compliance | 1 |
| 1.2. | Administrative Affiliation | 1 |
| 1.3. | Purpose, Application and Scope | 1 |
| 2. | Core Principles of Compliance | 2 |
| 2.1. | Mission Statement | 2 |
| 2.2. | Key Principles | 2 |
| 3. | Compliance Department Role | 3 |
| 3.1. | Compliance as a Second Line of Defence | 3 |
| 3.2. | Responsibilities | 3 |
| 3.2.1. | Business Conduct Compliance | 3 |
| 3.2.2. | Financial Crime Compliance | 4 |
| 3.2.3. | Compliance Assessment | 4 |
| 4. | Key Risks for Compliance Management | 5 |
| 4.1. | Compliance Risks | 5 |
| 4.2. | Risks with Compliance Elements | 5 |
| 5. | Third Party Compliance | 6 |
| 5.1. | Third Party Due Diligence | 6 |
| 5.1.1. | Scope of Investigation | 6 |
| 5.1.2. | Categorization of Risk | 7 |
| 6. | Sanctions Compliance | 9 |
| 6.1. | The LIA's Current Sanctions Regime | 9 |
| 6.2. | Sanctions Policy | 9 |
| 6.2.1. | Types of sanctions | 10 |
| 6.2.2. | Screening procedures and covenants | 11 |
| 7. | Reporting | 12 |
| 8. | Review of Policy | 12 |
| 9. | Appendix | 13 |
| | Definitions | 13 |



1. Introduction

The set of guidelines contained in this document form the basis of the Libyan Investment Authority's ("LIA") Compliance Policy. They set out the responsibilities and guiding principles of the Compliance Department.

1.1. Nature and Objectives of Compliance

Compliance can be defined as the state of adherence to applicable laws, regulations, guidelines, and best practice standards.

The core of LIA's Compliance Department is safeguarding the LIA by minimising its exposure to compliance risks. It will achieve this by delivering robust and pragmatic compliance advice and review services to the whole organisation, and through associated policies such as the Code of Conduct instil a culture of compliance across all employees.

1.2. Administrative Affiliation

The Compliance Department shall report directly, in organisational terms, to the Risk & Compliance Directorate of the LIA, and shall also maintain active relations with the various stakeholders of the LIA:

- It assists the Board of Directors ("BoD") and the Chief Executive Officer ("CEO") to ensure the LIA abides by relevant laws and regulations;
- It advises the BoD and CEO on LIA-wide compliance issues;
- It oversees the conduct of business and support functions;
- It develops and implements compliance risks and controls framework; and
- It shall cascade compliance best practices and awareness to the LIA's subsidiaries and portfolio companies in which the LIA has a controlling interest i.e. holds more than 50% of their capital.

1.3. Purpose, Application and Scope

The purpose of the Compliance Policy is to provide guidance on the function, role and activities of the Compliance Department. This policy outlines the role and function of the Compliance Department and its relation to other parties inside the LIA, as well as the specific compliance guidelines the LIA must follow when dealing with external parties. All Compliance personnel should ensure they read and are familiar with the contents of this Policy.

This policy complements the LIA's Code of Conduct, which covers guidelines on topics such as Conflicts of Interest, Market Conduct, Personal Dealing, Benefits, Hospitality and Gifts, Bribery and Corruption, Information Management and Whistleblowing. This policy and its dissemination and adoption is owned by the Compliance Department and should be familiar to all LIA staff.



2. Core Principles of Compliance

2.1. Mission Statement

“Everything we do, in providing a suite of compliance services – advising, reviewing, investigating and resolving issues – is designed to ensure that the LIA conducts business lawfully, fairly and ethically in the markets that it operates in”

The LIA’s Compliance Department exists to assist the Management in fulfilling its obligation to operate the LIA and all of its Subsidiaries in a sound and sustainable manner and in compliance with applicable laws, regulations and rules in all relevant jurisdictions.

2.2. Key Principles

The Compliance Department’s mission is supported by five key principles:

| | |
|---|--|
| <i>Compliance with legal and regulatory requirements</i> | The Compliance Department shall establish standards to meet minimum legal and regulatory requirements in all the jurisdictions in which the LIA operates. |
| <i>Culture of Compliance</i> | The Compliance Department shall promote a culture of Compliance across the LIA and within its investment portfolios. |
| <i>Portfolio Governance</i> | The Compliance Department shall work with the LIA’s Investment Directorate and other LIA departments, leading on the governance of the investment portfolios and subsidiaries from a compliance perspective. |
| <i>Continuous Oversight</i> | The Compliance Department shall construct a risk-based ongoing review programme in order to prevent or mitigate reputational risk to the LIA. |
| <i>Best Practice Adherence</i> | The Compliance Department shall regularly assess its adherence with the Santiago Principles and alignment with Sovereign Wealth Fund best practices. |



3. Compliance Department Role

3.1. Compliance as a Second Line of Defence

The LIA adopts a “three lines of defence” approach, which delineates the roles between functions in order to ensure effective risk management and control within the organisation. The first line of defence is the LIA’s Business Operations (conducting its business), the second line of defence is Risk and Compliance (monitoring / controlling risks), and the third line of defence is the Internal Audit Directorate (conducting an independent assessment).

The Compliance and Risk Departments provide oversight of business processes and they control and monitor risk. Compliance serves both as an advisory role to the business, assisting the business to design and implement business procedures and risk-mitigating controls to ensure compliance with regulatory requirements, and as a second level control function to execute (second line of defence), to implement, monitor and test certain first level business controls (first line of defence). Specifically:

- The Compliance Department is an oversight Control function, similarly to the Risk Management Department.
- Objectives of the Compliance Department are the following:
 - Advising on and overseeing accountable areas;
 - Reviewing controls environment;
 - Stewardship of company-wide compliance policies (such as the Code of Conduct);
 - Independently investigating and resolving incidents across the LIA.
- The Audit, Risk & Compliance Committee (“ARCC”), on behalf of the Board, oversees and evaluates the effectiveness of the Compliance Department.

3.2. Responsibilities

The responsibilities of the Compliance Department fall under three main categories, detailed in this section:

- Business Conduct Compliance
- Financial Crime Compliance
- Compliance Assessment

3.2.1. *Business Conduct Compliance*

The Compliance Department shall be responsible for:

- Setting the overall business conduct compliance framework;
- Developing, maintaining and assessing compliance with the LIA Code of Conduct and its guidelines on Anti-Bribery & Corruption, Gifts and Hospitality, Conflict of Interests, Personal Account Dealing, amongst others;



- Promoting business conduct compliance awareness across all departments and leading regular knowledge-sharing sessions ensuring all members of staff are adequately trained and certified;
- Reviewing and updating the suite of policies owned by the Compliance Department; and
- Managing any material breaches raised by individuals or departments.

Note: details of Personal Conduct are covered by the Code of Conduct and any violations of the Conduct will be reviewed by the Compliance Department.

3.2.2. Financial Crime Compliance

The Compliance Department shall be responsible for:

- Setting overall financial crime compliance framework and related policies (related policies including but not limited to the Sanctions Policy, Disclosure Policy and relevant areas of the LIA Code of Conduct).
- Recommending decisions regarding sanctions and ensuring compliance with imposed sanctions.
- Monitoring and reporting on compliance with risk limits regularly.
- Performing counterparty due diligence on potential vendors and investment venture partners as part of procurement or investment process.
- Promoting financial crime compliance awareness across all LIA departments and conducting regular knowledge-sharing sessions.

3.2.3. Compliance Assessment

The Compliance Department shall be responsible for:

- Ensuring the LIA is compliant with all applicable laws and regulations.
- Running periodic compliance risk self-assessment exercises (in alignment with other non-financial risks) and reporting outcomes.
- Ensuring any new procedure is vetted from the Compliance Department and ensuring monitoring is competent.
- Carrying out ongoing and permanent monitoring and reporting of compliance with policies, distinct from periodic monitoring, by working closely and intensively with other departments to identify the compliance implications of their policies and to work on implementing the controls and procedures established to monitor adherence to those policies.
- Performing key control and assessment activities of compliance risks including all LIA's business' and support function's compliance.
- Reviewing best practice and LIA performance against them (e.g. Santiago Principles).
- Tracking possession of privileged or price-sensitive information with clearly defined lists.



4. Key Risks for Compliance Management

As part of its mandate, the Compliance Department shall support in monitoring, preventing and mitigating risks to the LIA, as outlined below.

4.1. Compliance Risks

Compliance risk can be defined as the risk of legal sanctions, material financial loss or reputational loss that the LIA may suffer as a result of failing to comply with laws and regulations, its internal policies or its Code of Conduct and ethical standards.

Examples of compliance risk include, but are not limited to:

- Market abuse;
- Insider trading, including personal trading violations;
- Organisational conflicts of interest that are not properly mitigated;
- Inappropriate or illegal sales and trading conduct;
- Conflicts of interest resulting from inappropriate or excessive gifts or entertainment;
- Money laundering or terrorist financing relating to third party engagement (Section 5); or
- Engaging with parties in sanctioned countries (Section 6).

For more detail on guidelines of behaviour concerning the above points, please refer to the Code of Conduct.

4.2. Risks with Compliance Elements

Other types of risks include strategic, financial, technology or other risks that affect the LIA and may have, as a result, implications for Compliance. Examples of risks with compliance elements include, but are not limited to:

- Cybersecurity breach
- Counterparty relationships risk
- Data loss
- Personal risks
- Internal or external fraud



5. Third Party Compliance

The LIA is a global investor and, as such, must adhere to the highest international standards concerning its affiliation with any organisation or individual in order to build and maintain a trusted and prestigious reputation. The application of such standards concerns parties with which the LIA has relations through its investments, as well as any party from which the LIA procures goods and services. Furthermore, the policy applies both in the selection of potential new partners and in the monitoring of existing partners.

As a general principle, the LIA must not be involved or affiliated with any party (i.e. organisation or individual) that is associated with any economic crime. This includes but is not limited to: money laundering, terrorist financing and bribery.

5.1. Third Party Due Diligence

Due diligence can be defined as the set of investigation procedures used to assess whether an individual or organisation is suitable to becoming a business partner of the LIA. Such procedures must be activated prior to any business dealings with third parties.

Among the many types of due diligence procedures that may be put in place with third parties, the ones highlighted in this section have the objective of avoiding association with parties that condone or engage in economic crimes, which might impair the LIA's reputation.

Any breach of this policy may lead to specific investigation by regulatory authorities of the individuals involved and of the LIA as an organisation.

Due diligence must be conducted on any party in which the LIA invests or conducts a transaction with, regardless of whether the contact is initiated by the LIA or by the third party.

Only after a complete investigation and due diligence has been made, and no substantial risks have emerged, can the LIA activate business plans or engage in business transactions with the third party.

Any investigation and due diligence must determine two elements prior to beginning the investigation:

- The Scope of Investigation (Section 5.1.1.); and
- The Categorisation of Risk (Section 5.1.2.).

5.1.1. *Scope of Investigation*

The types of investment-related parties that are assessed before engaging in transactions include, but are not limited to, the following:

- Transactional third parties;
- Joint venture parties;
- Investment targets;



- Financial institutions (e.g. investment banks); and
- Lobbying firms or any other parties that provide support to the investment process.

The types of non-investment-related parties that are assessed before engaging in transactions include, but are not limited to, the following:

- Service Providers; or
- Vendors.

The Compliance Department has the right to initiate independent screening on third party organisations or individuals. Specifically, if the Compliance Department has any concerns about the third party either before or during their engagement, they may:

- Request that the third party completes a risk assessment questionnaire;
- Request a face-to-face meeting with the third party to discuss concerns and ask further questions;
- Suspend any further action pending investigation;
- Commission a report from a private investigator;
- Stipulate that additional anti-bribery and corruption provisions are included in the terms & conditions of the proposed contract of the engagement; or
- Decline to authorize the proposed engagement.

5.1.2 *Categorization of Risk*

The level of compliance risk can be categorized based on different variables.

Examples include:

- Categorisation based on geography¹:
 - Low risk countries e.g. Australia, Germany, France, Italy, Malta, US, UK, etc.
 - Medium Risk countries e.g. Brazil, China, Malaysia, Turkey, Tunisia, etc.
 - Severe risk countries e.g. Somalia, Syrian Arab Republic, Yemen, etc.
- Categorisation based on type of association:
 - Low risk² association (in low-risk territories):
 - Members of regulated professions (e.g. lawyers, accountants);
 - Public companies listed on a recognized stock exchange;

¹ Risk classification of countries relies on the World Bank Worldwide Governance Indicators (“WGI”). This index uses six factors to assess country risk: voice and accountability, political stability and absence of violence and terrorism, government effectiveness, regulatory quality, rule of law and control of corruption. The list should be reviewed and updated on an annual basis

² In the absence of other circumstances that give rise to a concern.



- Regulated companies: Companies whose activities are subject to regulatory oversight (with the regulator based in a low risk territory);
- Government bodies; or
- Any Government entity or company in which the Government has a controlling stake.
- High risk type of association:
 - Persons or close family members of persons with influence over the LIA or its subsidiaries;
 - Entities or companies related to the LIA either through ownership or provision of services to the LIA or subsidiaries;
 - Partners, principals, shareholders or employees of the LIA's external auditor; or
 - Any party who has meaningful ties with the LIA's external auditor.

The LIA shall not engage with any third party that is known or suspected to be:

- Paying or accepting bribes or other corrupt practices; or
- Engaged in money-laundering or other forms of financial impropriety.

Furthermore, certain circumstances may allow the Compliance Department to prohibit initial interaction based on a compliance risk assessment. These include but are not limited to the following:

- Undertakings with non-standard fee arrangements;
- Individuals acting as introducers on behalf of others; and
- Firms not willing to participate through a competitive tender process.



6. Sanctions Compliance

The LIA must operate in accordance with the sanctions regime currently imposed on a large part of its assets (Section 6.1).

Furthermore, the LIA shall comply with a series of international sanction regimes regarding its investments and engagement with third parties (Section 6.2).

The LIA must ensure full compliance with the sanction's regime imposed (throughout its duration) when carrying out its business. It should also account for international sanctions regimes such as the European Union sanctions and US sanctions when doing business with third parties.

6.1. The LIA's Current Sanctions Regime

A large proportion of the Libyan Investment Authority's assets are currently frozen in accordance with United Nations Security Council resolutions imposed in 2011 in order to safeguard Libya's assets at that time. The United Nations Security Council ("UNSC") Resolution 1970 of 2011 was passed, which aims to protect the LIA's internationally held assets. Both the UN and EU now apply these financial sanctions.

The LIA must comply with the UN sanctions regime in full and as stipulated in its provisions. The LIA may sometimes request licenses from regulators that allow for exceptions to sanctions or regulations. In these circumstances, it is the Compliance Department's responsibility to request and manage the licenses from regulators.

6.2 Sanctions Policy

The LIA shall comply with all trade and economic sanctions, laws and regulations that apply to its investments.

The sanction regimes most relevant to the LIA are the following:

- United Nations Security resolutions ("UN sanctions");
- US primary, secondary and sectoral sanctions ("US sanctions"); and
- European Union sanctions ("EU sanctions").

By doing so, the LIA reduces its reputational risk and reassures the third parties with which it engages. For this reason, all employees of the LIA must ensure that all investments, financing activities or other business activities comply strictly with these sanction regimes.

Any breach of these regulations may lead to multi-billion-dollar fines as well as heavy reputational impacts that may jeopardize the LIA's investment strategy.



6.2.1 Types of sanctions

The LIA will update this policy, in accordance with any changes in the aforementioned sanction regimes.

Sanctions can be categories in the following groups, outlined below:

- Geographic-based sanctions;
- List-based sanctions;
- Sectoral sanctions; and
- US secondary sanctions.

6.2.1.1 Geographic-based sanctions

These sanctions prohibit dealings that involve individuals or organisations that are located in a sanctioned country, defined as an “embargoed territory”. And hence the LIA is prohibited from making any transactions with any of the countries included in the US sanctions list.

6.2.1.2 List-based sanctions

These sanctions prohibit dealings involving individuals or organisations on a list.

Examples of these lists can be found in the following:

- The US list of Specially Designated Nationals or Blocked Persons (SDNs); or
- The EU Asset Freeze List.

6.2.1.3 Sectoral sanctions

These sanctions, introduced as a response to Russia’s activity in Eastern Ukraine and Crimea, prohibit transactions involving Russia’s finance, energy and military sectors.

6.2.1.4 US secondary sanctions

Specific sanctions are applicable to any non-US organisation that is involved in dealings with Iranian SDNs, Russian SDNs, North Korea or North Korean SDNs, or Hezbollah.



6.2.2 Screening procedures and covenants

Prior to dealing with any entity of a sanctioned country³, employees must notify the Compliance Department and cease any activity around the transaction until the Compliance Department has reviewed the situation.

Transactions involving sanctioned countries are strictly forbidden, unless written clearance for the transaction is given by the Compliance Department.

Before the LIA engages in a new transaction, all parties shall be screened against the aforementioned lists (e.g. SDN, EU Asset Freeze List). This includes:

- Proposed borrowers;
- Acquisition targets;
- Co-investors; and
- Joint venture partners.

The Compliance Department shall also investigate whether the parties are owned by a sanctioned individual or organisation. If the investigated party is a sanctioned party or is owned for more than 50% by a sanctioned party, further investigation will be carried out.

In certain cases, the LIA may agree to covenants about the LIA's compliance with sanctions.

³ This includes embargoed territories, countries subject to sectoral sanctions and countries subject to list-based sanctions.



7. Reporting

The Compliance Department shall submit, together with the Risk Management Department, a quarterly Risk & Compliance report to the ARCC.

This Risk & Compliance report shall include:

- Risk profile reporting (competence of the Risk Management Department)
- Risk metrics and forecast (competence of the Risk Management Department)
- Compliance risk assessments and mitigation (competence of the Compliance Department)
- Compliance with regulations (competence of the Compliance Department)

8. Review of Policy

The Director of Compliance shall submit the Compliance Policy to the Director of Risk and Compliance for review, who shall refer it to CEO for initial approval. The CEO shall then recommend it to the ARCC for review and submission to the BoD for approval.

"A large proportion of the Libyan Investment Authority's assets are currently frozen in accordance with United Nations Security Council resolutions imposed in 2011.

The ARCC shall determine and monitor appropriateness and effectiveness of the LIA's Compliance framework, policies and practices on an annual basis.

The Director of Compliance is responsible for implementing this policy, as it is assumed that this policy accurately represents the framework and procedures in place and that those are updated as required.

In the case of any unclear or ambiguous wording in the Arabic version of the Policy, the English version shall prevail.



9. Appendix

Definitions

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

- “Board” or “BoD” refers to the LIA’s Board of Directors
- “Compliance” refers to the LIA’s Compliance Department
- “Employee” means any person working for the LIA and includes full time, part time, probationary, contract/temporary staff, trainees or consultants at the LIA, as well as the Compliance officers and other senior managers within the organisation
- “LIA” or “the LIA” refer to the Libyan Investment Authority
- “Subsidiaries” or “LIA’s subsidiaries” means any subsidiary of the LIA including LTP, LAP, LAFICO, LLIDF and Oilinvest, amongst others