

Finabank Integrity Framework

2020



Version Management

Document	FinaBank Integrity Framework
Version	V0.1
Date	June 2020
Owner	Office of Institutional Integrity and Legal Affairs
Author	Farashja Ozir-Ghazi

Change Management

Version	Date	Editor	Description
V0.1	12 June 2020	Eblein Frangie Samseerali Sheikh Alibaks Farashja Ozir-Ghazi	

Approved by

Version	Date	Name	Job title	Signature
V01		Eblein Frangie	CEO	
V01		Feroz Ishaak	Chairman of the RC of the supervisory board	<i>F.M.S. Ishaak</i>

Table of Contents

List of Abbreviations	5
Introduction	6
Section 1 Compliance Risk Management Charter.....	7
1. Compliance Risk Management Strategy.....	8
1.1 Mission of the Compliance Risk Management Function.....	8
1.2 Purpose of the Compliance Risk Management Function.....	8
2 Definition and Scope of Compliance Risk	9
2.1 Compliance Risk.....	9
2.2 Integrity and Reputation Risk.....	9
2.3 Compliance Risk Identification method - SIRA.....	10
2.4 Beyond the scope of Compliance Risk.....	10
3. Compliance Risk Management Roles & Responsibilities.....	11
3.1 Responsibilities of the Board of Directors	11
3.2 Responsibilities of all Employees.....	11
3.3 Responsibilities of the Junior Manager Institutional Integrity Officers	11
3.4 Responsibilities of the Manager OIILA.....	12
4.1 Independence	13
4.2 Investigate and challenge	13
4.3 Escalation	13
4.4 Access	13
4.5 Liaison and partnering	13
4.6 Capabilities, Evaluation and Remuneration	14
4.7 Appointments and Terminations	14
5. Reporting.....	15
5.1 Reporting lines Compliance Management Function.....	15
5.2 Reporting lines Organization regarding Compliance	15
5.3 Organizational structure of OIILA.....	16
Section 2 Compliance Risk Management Framework	17
6. The Vision, Mission and Core Values of FinaBank.....	18
7. The Three lines of Defence model.....	19
8. Key components of the Framework and the Chart.....	20
8.1 The Chart and the Key activities	20
8.2 Identification of Compliance Obligations.....	20
8.3 Risk Assessment.....	20
8.4 Compliance Risk Mitigation.....	21
8.4.1 KYC-CDD Policy	21
8.4.2 Whistleblower Policy	21
8.4.3 Anti-Bribery and Anti-Corruption Policy	22

8.4.4	Conflict of Interest Policy.....	22
8.4.5	Tax Policy	22
8.4.6	Cash Handling Policy.....	22
8.5	Compliance Risk Monitoring.....	23
8.6	Compliance Risk Management Reporting.....	23
8.7	Compliance Risk Management Advisory.....	23
8.8	Training and Education.....	23

List of Abbreviations

OIILA	Office of Institutional Integrity and Legal Affairs
II	Institutional Integrity
ERMF	Enterprise Risk Management Framework
IAD	Internal Audit Department
KYC	Know Your Customer
LoD	Line of Defence
RC RvC	Risk Committee of the Supervisory Board
RCC	Risk and Compliance Committee
RMD	Risk Management Department
SB	Supervisory Board
SIRA	Systematic Integrity Risk Analysis

Introduction

Trust is one of the key elements of FinaBank's core values. It is of the utmost importance that our stakeholders and the community we operate in can rely on us to act responsibly. Managing compliance risks effectively builds trust and is our social license to operate. It is the bank's duty to manage the integrity risks and keep the integrity of the system intact. In doing so, the bank complies with its gatekeeper's function.

To help our business manage Compliance Risks effectively, FinaBank has adopted the Compliance Risk Management Charter and Framework. The Charter sets out the roles and responsibilities and the Framework is the tool for the FinaBank employees to manage Compliance Risks.

Section 1 Compliance Risk Management Charter

This Charter applies to all Finabank employees and its purpose is to lay out the roles and responsibilities of Compliance Risk Management within our bank.

1. Compliance Risk Management Strategy

Managing our Compliance Risks effectively builds trust and credibility for FinaBank. Integration of Compliance Risk Management into our strategic planning process and into our daily business helps us to take the necessary actions to protect our reputation, which gives us a competitive advantage.

1.1 Mission of the Compliance Risk Management Function

The mission of the Compliance Risk Management Function is to create an appropriate path to strategic success, by fully integrating compliance risk management into daily business activities and strategic planning of FinaBank. While integrity is the responsibility of all, the Compliance Risk Management Function will help the business navigate through complexities and provide timely education, advice and solutions.

1.2 Purpose of the Compliance Risk Management Function

The Compliance Risk Management Function operates within the Enterprise Risk Management Framework (ERFM) with focus on identification, prevention, monitoring and detection, resolution and advisory. Specific emphasis is laid on:

- Facilitating the effective identification of risks relating to violation of relevant external requirements, such as compliance with laws and regulations, as well as providing advice on risk reduction measures.
- Developing and facilitating the implementation of internal controls that will provide the organization with protection from compliance risk.
- Monitoring and reporting on the effectiveness of control measures.
- Providing the business with advice regarding acceptable behaviour and practices in relation to the interpretation of external and internal laws and regulations.
- Monitoring relevant regulatory developments within the compliance function's areas of responsibility.
- Ensuring awareness and training.

2 Definition and Scope of Compliance Risk

2.1 Compliance Risk

Compliance is defined as the outcome of adhering to a rule. Compliance risk captures the legal and financial penalties for failing to act under internal and external regulations and legislature. To be able to comply, the rules and regulations are clearly defined, and the following are considered:

- Regulation or act
- Penalties for non-compliance
- Obligation and invested parties
- Risk rating
- Compliance status

Compliance risk management should:

- understand what actually constitutes a non-compliance risk for the bank.
- understand the bank's tolerance as regards a compliance risk.
- ensure that the bank's compliance processes keep pace with compliance risks.

The failure to identify compliance risks may lead to integrity risk and reputational damage.

2.2 Integrity and Reputation Risk

To manage a comprehensive compliance program, integrity risk is an important element. Integrity risk refers to the threat to the reputation and profitability of the business due to people-related incidents such as misconduct, bullying and sexual harassment, anti-competitive behaviour, bribery and corruption, inappropriate use of social media, breaches of privacy, conflicts of interest, fraud and whistle blower abuse.

Integrity is the main focus in managing the compliance risks of the bank and therefore Compliance Risk is often referred to as Integrity Risk. Reputation Risk however is not the same as Compliance Risk because reputational damage is only one possible outcome of compliance risk.

2.3 Compliance Risk Identification method - SIRA

Compliance risks within the bank are identified with a Systematic Integrity Risk Analysis – SIRA (The SIRA is explained in 7.3).

The SIRA resulted in the following integrity risks and control measures:

Risks	Control Measures									
	1LoD								2LoD	3LoD
	1. CDD/KYC framework	2. client screening framework	3. transaction monitoring framework	4. transaction screening framework	5. IT security policy	6. business procedure framework	7. employee integrity policy	8. policy framework	9. compliance monitoring program	10. audit
Money Laundering	x	x	x	x		x		x	x	x
Terrorist Financing	x	x	x	x		x		x	x	x
Sanction evasion	x	x	x	x		x		x	x	x
Tax non-compliance	x		x	x				x		x
Bribery	x						x	x	x	x
Corruption	x						x	x	x	x
Conflict of Interests							x	x	x	x
Employee							x	x	x	x
Fraud						x		x		x
Cybercrime					x					x

2.4 Beyond the scope of Compliance Risk

Compliance with laws, regulations and standards that relate to the following support functions fall beyond the scope of the Compliance Risk Management Function:

Risk Type	Support Function
Financial and Tax	Accounting and Reporting Treasury management
Credit	Credit Risk Management Legal
Market	Market Risk Management
Operational	ICT Human Resources Facility Management (GA)

These risks are the first line responsibility. They are not managed by OIILA, but are monitored in the ERMF.

3. Compliance Risk Management Roles & Responsibilities

3.1 Responsibilities of the Board of Directors

The Executive Board of Directors (the Board) is the owner of the Compliance Risk Management Function within FinaBank. They should lead by example and set the tone for creating trust and ensuring that the Bank complies with all relevant laws and regulations applicable to FinaBank.

To supervise the effective management of all risks within Finabank, a separate Risk Committee has been set up within the Supervisory Board.

The Board appoints one of its members as Chief Financial Risk Officer (CFRO). The CFRO oversees the Compliance Risk Management Function, which is embedded in the Office of Institutional Integrity and Legal Affairs (OIILA) led by the Manager OIILA.

A Risk and Compliance Committee (RCC) has been set up as an additional measure, because of the importance of effective risk management. The Board, OIILA and the Risk Management Department are part of this Committee.

The Board must create an environment within the bank, in which the importance of meeting compliance obligations, including FinaBank Business Principles, is well understood. This is achieved by providing sufficient resources (training, budget, staffing, etc.) to the Compliance Risk Management Function.

3.2 Responsibilities of all Employees

Every employee has the responsibility to manage compliance risk and to comply with applicable laws, regulations and standards. The Board has to ensure that every employee is aware of the compliance requirements they need to implement on a daily basis and each employee is obliged to comply with such requirements. Management has a program to judge the performance of each employee against the compliance requirements.

3.3 Responsibilities of the Junior Manager Institutional Integrity Officers

The Junior Manager Institutional Integrity must:

1. manage and coach the Institutional Integrity (Senior) Officers (day-to-day operations management)
2. determine which laws and regulations apply to the bank and which should be areas of attention for OIILA (List work area / framework).
3. conduct an SIRA.
4. translate the laws and regulations into internal policies and procedures. A collection of these must be incorporated in the bank's integrity policy.
5. promote awareness with regular awareness training, etc.
6. supervise compliance with the integrity policy. This includes the daily activities of Institutional Integrity (II), including the reporting activities.

7. report compliance with the integrity policy and procedures to the Board, the Risk and Compliance Committee (RCC) and the Risk Committee of the Supervisory Board.
8. give advice on policy issues.

3.4 Responsibilities of the Manager OIILA

The Compliance Manager must:

1. develop integrity and governance policies to support the bank's strategy.
2. annually contribute to the bank's business plan and the implementation of the resulting projects.
3. develop the annual plan of the department and ensure that it is implemented.
4. monitor, identify and report integrity risks, as well as give advice and make recommendations regarding integrity issues to manage, mitigate or eliminate risks.
5. monitor and ensure that the integrity and governance policy is in line with existing national and international laws and regulations.
6. analyze the impact of new or changing national and international legislation on business operations and make recommendations for adapting existing processes.
7. conduct tests, in which the effectiveness of the existence, design and operation of the control measures regarding integrity and governance are at risk.
8. make the bank aware of all integrity risk-related issues.
9. report to the Board, the RCC and the RC of the Supervisory Board.

4. Authority and Capabilities of Compliance Risk Management Function

4.1 Independence

Objectivity and independence are essential to the effectiveness of the Compliance Risk Management Function. This means that OIILA can do its work independent of the daily first line activities and independent of the functions that account for commercial and financial performance. This objectivity and independence of OIILA is guaranteed by the direct reporting line of OIILA to the RCC and the RC of the Supervisory Board.

The importance of the department is to be able to monitor compliance with both national and international laws and regulations, policies and procedures, in order to continue guaranteeing the integrity of the bank. The department functions as a "second line of defence" and is therefore not positioned as a line department, but as a staff department.

4.2 Investigate and challenge

When an II Officer identifies an integrity risk, the officer has the authority to investigate the risk and should not be limited to conduct the investigation in detail. If the problem is not resolved, the officer must use the escalation procedure.

4.3 Escalation

The II Officer uses the escalation procedure by informing the Junior II Manager about the risk. Together with the II Officer, the Junior II Manager must decide if the integrity risk needs to be escalated to the Manager OIILA. If the integrity risk is unacceptable the RCC needs to be involved. The Manager OIILA presents the case to the RCC where a decision is made on the matter in the Committee.

4.4 Access

The Manager OIILA, The Junior Manager II and the II Officers must have direct access to all the areas of their responsibilities. This includes all information about e.g. employees, systems, the Board (including the CEO) and the Supervisory Board.

The Manager OIILA, The Junior Manager II and the II Officers must have the opportunity to attend relevant Board and Committee meetings (e.g. RCC meeting, Managers meeting, RC meeting) and have a say to raise any important/relevant matter.

4.5 Liaison and partnering

The bank acknowledges that adequate cooperation and sharing responsibility between the business line and the assurance departments (OIILA, Risk Management Department and Internal Audit Department) is of great importance to ensure that the compliance risks are mitigated.

In addition, quarterly meetings are organized with the departments closely associated with compliance activities, as well as those with increased risks.

4.6 Capabilities, Evaluation and Remuneration

OIILA employees must have the necessary qualifications, certifications, experience, professional and personal skills to perform their work properly. An onboarding process is used for new employees, which includes a background check, an assessment and a certificate of good conduct. A fixed profile has been laid down by the Board of Directors and the Risk Committee of the Supervisory Board for the Manager OIILA. The Manager OIILA must have completed the required professional training. All OIILA employees must also have a good understanding of the operations of FinaBank and the obligations, legislations and standards that impact the Bank. To maintain expertise and to develop the skills of OIILA employees, ongoing training focused on banking, risk analysis, control techniques and standards is key.

- In order to limit loss of critical ability and objectivity, the principle of job rotation is applied in routine activities. Measures are taken to ensure that the necessary competence and expertise are not endangered. The policy with regard to the frequency, the manner in which and the conditions have been laid down. A cooling-off period is observed when officers of operational departments are transferred to OIILA and need to monitor their own activities or the processes in which they were involved.

The evaluation and remuneration of OIILA employees takes place in accordance with the performance management and remuneration policy in accordance with the HR manual. Exceptions to this only take place after consultation and approval by the Risk Committee of the Supervisory Board. The remuneration does not depend on the financial results of the department where it conducts the audits. When awarding performance awards, conflicts of interest and the risk of infringement of independence and objectivity are avoided.

4.7 Appointments and Terminations

The appointment, assessment and dismissal of an II Officer are initiated by the Junior II Manager after consulting the Manager OIILA. The Manager OIILA informs the Board about the appointment, assessment and dismissal of an II Officer.

(Voluntary) resignation of the Manager OIILA takes place on the basis of the procedure established by the bank, which states that such resignation will take place after clearly defined grounds have been established. The Risk Committee of the Supervisory Board will form an opinion on the resignation and the Board must take the opinion into account before the (voluntary) resignation becomes effective.

The appointment, assessment and dismissal of the Manager OIILA are done by the Board in consultation with the Chairman of the Risk Committee Supervisory Board.

5. Reporting

5.1 Reporting lines Compliance Management Function

The Reporting lines of the Compliance Management Function are as follows:

- The employees of Institutional Integrity report to the Junior Manager II.
- The Junior Manager II reports to the Manager OIILA.
- The Manager OIILA has a reporting line to the CFRO (administrative reporting line) in the Management Department meeting.
- The Manager OIILA reports monthly to the RCC and quarterly to the Risk Committee of the Supervisory Board (functional reporting line).

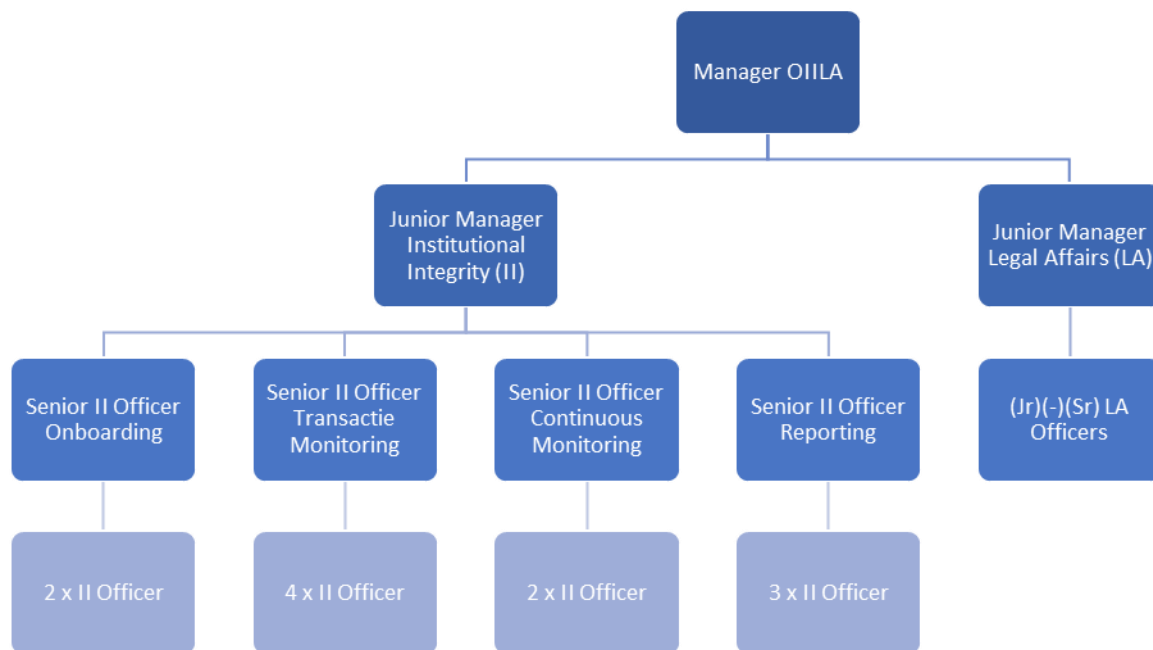
The report includes the statistics of daily monitoring, identified integrity risks to the bank, corrective measures and recommendations. Also included is the follow-up of previous recommendations and agreements made. To verify the findings these are discussed in advance with the manager of the relevant department.

5.2 Reporting lines Organization regarding Compliance

The organization has the option to raise compliance issues to OIILA through the following channels:

- E-mail, if it is about issues/advice from OIILA.
- The whistleblower form, if it is about a whistleblower report (e.g. internal fraud).
- The registration template, if it is about a business gift.
- The MOT form, if it is about a subjective report to the FIU Suriname.

5.3 Organizational structure of OIILA



The unit 'Onboarding' aims to identify the integrity risks associated with high risk customers and to formulate an advice on these customers, in order to mitigate the risk.

The unit 'Transaction Monitoring' aims to identify the integrity risks associated with customer transactions, to formulate advice on this in order to mitigate the risk and also draw up a monitoring plan for the customers with high risk transactions.

The unit 'Continuous Monitoring' aims to keep the files and information of customers in the system up to date and also to check that there are no changes in the customer profile or transaction profile of customers.

The unit 'Reporting' aims to maintain integrity with regard to reports to external parties and to conduct an analysis on this to determine whether customers' transactions are conducted with integrity.

Section 2 Compliance Risk Management Framework

The Compliance Risk Framework sets out the principles, processes and tools that all employees of FinaBank use to effectively manage Compliance Risks.

The FinaBank Vision, Mission, Core Values and the Three lines of Defence model are import building blocks of the Framework, which will be outlined further in the following chapters.

This Framework should be used in conjunction with the Charter set out in Section 1.

6. The Vision, Mission and Core Values of FinaBank

Vision

We are the number one financial solutions provider.

Mission

With our dedicated and caring professionals we successfully enable your ambitions financially.

Core Values

- Trust : We act responsibly
- Partnership : We work as one team
- Agility : We go the extra mile
- Innovation : We improve continuously
- Expertise : We are the best in class

The core values of FinaBank state what is important to the Bank, what FinaBank believes in and what it aims at. These core values are the soul of FinaBank. They are the foundation of our culture, day to day work and this Compliance Framework.

7. The Three lines of Defence model

To manage all risks, FinaBank uses the 'Three Lines of Defence model'. This model stated below is essential for the effective operation of the Compliance Framework.

1 st Line of Defence	2 nd Line of Defence	3 rd Line of Defence
Business management	Compliance and Risk Management	Internal audit
Functions that own and manage risks	Functions that oversee risks	Functions that provide independent assurance
Responsible for: <ul style="list-style-type: none"> developing and implementing mitigation activities, including monitoring and reporting, for managing Compliance risks in business activities own processes 	Responsible for: <ul style="list-style-type: none"> identifying relevant Compliance Risk-related laws, regulations and standards (in accordance with Legal). translating the laws, regulations and standards into compliance obligations. helping to identify the activities to mitigate risk within the bank's risk appetite. supporting, advising, coordinating and monitoring whether the "First Line of Defence" actually takes the responsibilities 	Responsible for: <ul style="list-style-type: none"> independently assessing the design, existence and operation of the processes and activities in the first and second lines and providing additional assurance on the quality of management and control to the Board of Directors and the Supervisory Board. operating completely independently of all other organizational units.

The added value of the cooperation between the different lines of defence is more than just the organizational structure and the naming of the roles. It is a fundamentally different way of working (collaborating) and thinking and thus contributes to strengthening the risk culture, taking responsibilities to manage risks and ultimately contributing to optimizing and integrating the integrity and risk functions within the bank.

8. Key components of the Framework and the Chart

FinaBank's Compliance Risk Management Framework consists of the Compliance Chart and Advisory. The Compliance Chart reflects all the laws and regulations FinaBank must comply with, the compliance obligations, the integrity risks and the responsibilities of the employees. Advisory Services regards the support and advice CMD gives in compliance related issues.

8.1 The Chart and the Key activities

The Compliance Chart is the guide for the first line to operate. The Chart includes the laws and regulations the bank must comply with. The Chart also lays down the compliance obligations, the integrity risks for the obligations, the policies/procedures in which the bank already has mitigations and the responsible department for the compliance obligations.

The Chart has the following key activities:

1. The laws and regulations the bank must comply with.
2. The compliance obligations resulting from the laws and regulations.
3. The integrity risks resulting from the compliance obligations.
4. The risk assessment as in the rating of the risks in high, medium and low.
5. The business processes on which the compliance obligations have an impact.
6. The policies/procedures of the bank which include mitigations.
7. The ownership of the processes, activities and compliance obligations included in the chart.

The Chart is a clear display of the compliance obligations and the responsibilities of employees and is included in appendix 1.

8.2 Identification of Compliance Obligations

The Chart is kept up to date, so the bank complies with all the relevant laws and regulations. In the Chart a clear display of the compliance obligations and the associated risks is determined, so the first line knows what the compliance obligations are, to include these in their daily business activities. The first line must do a risk-based due diligence. This is also important in assessing the effectiveness of a company's compliance program (a risk-based orientation). The compliance program of the bank must incorporate policies and procedures to have mitigations for the integrity risks. If a new law or regulation is implemented, the Chart must be updated. The OIILA must identify the new and updated laws and regulations and translate the compliance-related laws and regulations into compliance obligations.

8.3 Risk Assessment

SIRA

Determining the compliance risks resulting from the compliance obligations in the Chart is an ongoing process. The Systematic Integrity Analysis (SIRA) is the tool that is used within FinaBank to identify and analyse these risks to determine their nature and extent.

The SIRA is performed, based on the risk carriers and the risk areas. The SIRA shows the probability that a certain integrity risk will arise and what the mitigating measures for that risk may be. It can also

determine if the mitigating measures already taken by the bank are adequate and if additional measures need to be taken.

ERMF

The Enterprise Risk Management Framework is the High-Level Risk Framework that Finabank uses to manage its risks. It is essential that all the high compliance risks are included in the ERMF register with all mitigating control measures mentioned. The Risk Management Department will monitor the Key Risk Indicators for all high ranked risks to be able to proactively manage these risks.

Detailed risk assessment

To manage compliance risks the bank also performs detailed risk assessments while onboarding new clients. A risk analysis of the client is performed, to determine the risk rating of a client (as in low, medium and high). This is about the identification of the potential risks a client has and the outcome determines the type of risk mitigation and monitoring. The monitoring can be on transactions (Transaction Monitoring) and on periodic review of the client (Continuous Monitoring).

If necessary, an enhanced due diligence is conducted to determine the potential risks a client has. More detailed information is requested to determine the risk profile of the client. If the client poses a risk to the bank, the RCC must decide if the risk is acceptable or not and take a decision to onboard the client.

8.4 Compliance Risk Mitigation

Mitigation of risks is done by implementing control measures like implementation of standards, policies, procedures and guidelines. Based on the SIRA the Bank has established the following six (6) policies to mitigate key integrity risks.

8.4.1 KYC-CDD Policy

The KYC-CDD policy (Know Your Customer / Client-Customer Due Diligence) relates to the "Know Your Customer" principle, which emphasizes the importance of the bank always being aware of with whom it does business. Application of KYC is a fundamental aspect of keeping integrity within the bank in order to protect it primarily against any act related to money laundering and terrorist financing. The bank's KYC-CDD Policy is therefore designed to minimize the risks that customers entail, such as reputation risk and liability risks. The aim of the KYC-CDD Policy is to contribute to an adequate understanding of the bank's potential customer from a risk-bearing perspective.

8.4.2 Whistleblower Policy

The bank strives to adhere to the highest standards of ethical, moral and legal behaviour. To maintain these standards, the bank encourages its employees who have complaints or concerns about alleged misconduct or irregularities to report them without any fear for sanctions or retaliation.

This Whistleblower Policy supplements the Bank's Code of Conduct and Integrity and contains guidelines that generally describe and prescribe the behaviour expected from employees. Bank employees attest to their compliance with the policy as part of the annual recognition and certification of compliance with the Code of Conduct and Integrity.

8.4.3 Anti-Bribery and Anti-Corruption Policy

The bank is bound by national and international laws and regulations to ensure that anti-bribery and anti-corruption laws are adhered to and constitute the basis for its business activities. The bank makes every effort to do this in a legal and ethical manner. As part of this commitment, all forms of bribery and corruption are unacceptable and will not be tolerated.

This policy supplements the Code of Conduct and Integrity, as included in the Corporate Governance Handbook and the Bank's Human Resource Handbook. Stakeholders are not concerned with bribery and corruption and promote the de-risking or refusal of any customer suspected of being guilty of doing so. The bank has developed the Anti-Bribery & Anti-Corruption policy to help employees identify when something is prohibited, so as to avoid bribery and corruption, as well as guidance on how to deal with it issues.

8.4.4 Conflict of Interest Policy

The bank is committed to the relationship we have with our customers and suppliers and we act with integrity, honesty and professionalism in accordance with our interests. Therefore it is important to have a policy about conflicts of interest, how to deal with these conflicts.

Conflict of Interest is any situation in which:

- a provider or representative has an actual or potential interest that, when providing a financial service to a customer and suppliers, may affect the objective performance of his / her obligations to that customer; or
- a provider or agent is prevented from providing unbiased and fair financial services to that client or acting in the best interest of that client, including (but not limited to) financial ownership, or any relationship with a third party.

8.4.5 Tax Policy

This policy indicates which control measures the bank takes under the FATCA laws and regulations relating to tax offences in order to mitigate the integrity risks. The bank has to comply with the FATCA laws and regulations to capture tax evasion. If the bank doesn't comply with the FATCA laws and regulations, sanctions may be imposed on the bank (for example a fine).

Tax risks related to the above may be divided into tax avoidance (the legitimate minimization of taxes) and avoidance through tax evasion (the illegal practice of not paying taxes).

8.4.6 Cash Handling Policy

This policy describes the discouragement of cash and the tracking of money (the trail of money). Cash carries more risks, as there can always be questions about the origin of the funds. This is to prevent parties from concealing the origin of criminal activities, especially money laundering by organizations involved in the illicit trade in goods.

8.5 Compliance Risk Monitoring

Monitoring of Compliance Risks helps FinaBank to be certain that mitigation measures work adequately and to identify new or changed risks. Monitoring also helps to assess if the compliance risks don't exceed the Risk Appetite of the Bank.

8.6 Compliance Risk Management Reporting

If material compliance risks occur that are not included in the ERMF risk register, OIILA needs to inform the Risk Management Department immediately so this could be included and shared with the Board and the RC of the Supervisory Board for strict monitoring.

Furthermore, OIILA reports on a monthly basis to the RCC and on a quarterly basis to the Risk Committee of the Supervisory Board.

8.7 Compliance Risk Management Advisory

OIILA has a proactive role in advising the Board, Committees and employees on compliance risks, compliance obligations, concerns and other compliance related issues.

8.8 Training and Education

The awareness and understanding of compliance risks must be part of the culture of the bank. It is important that employees must be aware and have a good understanding of the Finabank Compliance Charter and Framework. It is also essential that all employees understand the process for addressing compliance issues and the consequences of not meeting our compliance obligations.

Every year, a formal training plan is created in collaboration with the Human Resource Department, which includes all necessary training courses, training methods and target audiences. If necessary, additional courses may be added to the plan during the year.

The target groups for training activities are divided into:

- The Integrity and other assurance employees.
- The bank's employees (including the Board).
- The Supervisory Board.
- External parties who provide services to the bank.

Some of the Integrity Awareness training activities the bank engages in are listed below:

Type of training	Who	When
Onboarding Presentation OIILA	Each new employee	During the introduction week
Compliance Digital Learning Environment (DLO)	<ul style="list-style-type: none">• Each new employee• Each employee	<ul style="list-style-type: none">• Within one month after the onboarding• Annually
Compliance Awareness sessions	Each employee	Annually
Front face meetings	Business line departments (1LoD)	Once a quarter
Credit meeting	Managers of the Business line departments (1LoD)	Once a month
FIBA-AMLCA	Manager OIILA and all II	Once according to the PBM, then

	employees	maintain the certification through ongoing training
CPAML	Manager OIILA, Junior Manager II and seniors of II	Once according to the PBM, then maintain the certification through ongoing training