

Anti-Money Laundering and Counter-Financing of Terrorism Policy

Version	2.0
Latest update	01.04.2025
Previous update	22.04.2024
Next update	Q1 2026
Written by	MLRO (Compliance Officer) and reviewed by Legal Counsel
Approved by	Managing Director
Approval date	17.04.2025
Signature	<i>C. Drommond</i> Cornelia Drommond Oonincx as Proxy Holder eMoore N.V.

Table of contents

Table of contents	2
1. Introduction	4
2. Purpose, Compliance, and Scope	4
3. Applicability	4
4. Policy Review	4
5. Disciplinary Measures and Legal Consequences	5
6. Legal Framework for AML/CFT	5
7. Board Accountability	6
8. The Money Laundering Reporting Officer (MLRO)	6
8.1.1 MLRO Core Functions	7
8.1.2 MLRO Reports	7
8.1.3 Designated Employees	8
8.2 Fraud & AML Team	8
9. Training and Awareness	8
10. Money Laundering & Funding of Terrorism	9
10.1 Money Laundering	9
10.2 Funding of Terrorism	9
10.3 Other Financial Crimes	10
11. Reporting Obligations	10
11.1 Internal Reporting Procedure	10
11.1.1 Obligations	10
11.1.2 Timing	10
11.1.3 Additional Internal Reports	11
11.1.4 MLRO Responsibilities	11
11.1.5 MLRO Conflicts of Interest	11
11.2 Definition of a Fact	11
11.3 Contextual Clarification	11
11.4 Navigating Suspicion	12
11.4.1 Criteria for Reasonable Suspicion	12
11.4.2 Establishing Reasonable Grounds to Believe	12
11.5 Addressing Completed or Attempted Transactions	12
11.6 Recognising Unusual Activities - Red Flags	12

11.7 Protocol for External Reporting	13
11.9 Avoiding "Tipping Off"	13
11.10 Decision-making in Uncertain Circumstances	14
12. Customer's Data Collection & Processing	15
13. Risk-Based Approach (RBA)	15
13.1 Business Risk Assessment (BRA)	16
13.2 Customer Risk Assessment (CRA)	16
13.3 CRA Methodology	16
13.4 Risk Appetite	17
14. Politically Exposed Persons (PEP)	17
15. Internal Control Rules	18

1. Introduction

Comeback N.V. is a company registered under the laws of Curaçao and, in virtue of a transition period, it operates online gaming services whilst in the process of obtaining a Gaming License from the Curaçao Gaming Authority. Comeback N.V. shall be herein referred to as the “Licensed Company”.

The Licensed Company is dedicated to preventing money laundering and terrorist financing, and accordingly, this Anti-Money Laundering and Counter-Terrorist Financing Policy, coupled with internal procedures, constitutes a robust framework to deter illicit transactions. By aligning with applicable AML standards, the policy aims to reduce the risk of the Licensed Company’s inadvertent involvement in unlawful financial dealings.

All persons representing the Licensed Company must steer clear of money laundering or terrorist financing activities and promptly report any suspicions to the Money Laundering Reporting Officer (MLRO), without alerting individuals potentially under investigation.

2. Purpose, Compliance, and Scope

This policy provides a clear blueprint to assist relevant persons in mitigating risks tied to money laundering and terrorist financing. Beyond legal adherence, the objective is to minimize the risk of the operator's platforms being exploited for illegal financial dealings. It reflects the broader compliance strategy ratified by the operator’s top management and board of directors and emphasizes the duty to report violations to the relevant financial intelligence authorities or similar applicable bodies.

3. Applicability

All personnel and individuals in roles akin to staff, irrespective of their functions within the Licensed Company, are bound by this policy. This policy shall apply to the gaming operations of the Licensed Company in the manner detailed herein and as may be supplemented by ad hoc procedures.

4. Policy Review

This Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) Policy will be reviewed annually or when significant regulatory changes demand. Recommendations for improvements should be directed to the MLRO. The MLRO has the discretion to seek internal and/or external expertise when updating the policy and is tasked with regular reporting to the Licensed Company's management board (the "Board").

Major policy changes or introductions require approval from the top management and Board. The MLRO will notify staff of any updates through email and ensure accessibility via a shared digital platform.

5. Disciplinary Measures and Legal Consequences

Failure to comply with this policy can lead to disciplinary measures, including potential termination. Breaching AML reporting norms may be a criminal offence under applicable laws. Likewise, tipping off a customer under scrutiny is a direct violation of this policy and may result in a serious criminal violation in terms of applicable law.

6. Legal Framework for AML/CFT

This policy aligns with the rules applicable to the Licensed Company according to the laws of Curaçao.

Curaçao Framework - applicable to Comeback N.V.:

- National Ordinance on Games of Chance (LOK)
- Central Bank of Curaçao and St Maarten AML guidelines
- National Ordinance on identification when rendering services
- National Ordinance on the reporting of unusual transactions
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction issued by the Curacao Gaming Control Board (GCB) January 2025

For details on reporting and "tipping off," consult the relevant sections of this policy.

7. Board Accountability

The Board of the Licensed Company assumes collective responsibility for ensuring adherence to the AML/CFT regulations. The Board is entrusted with:

- Promoting a culture of compliance.
- Adopting a risk-based strategy to AML/CFT, crafting robust measures against potential risks.
- Assigning a competent individual as the MLRO and ensuring they are adequately resourced.
- Monitoring regular managerial reports on AML/CFT measures to understand the organisation's risk profile.
- Ensuring customer onboarding aligns with this policy.
- Overseeing and approving updates to the Business Risk Assessment (BRA).

8. The Money Laundering Reporting Officer (MLRO)

The Licensed Company consistently designates an individual of substantial authority as the Money Laundering Reporting Officer (MLRO). While the role is referred to as Compliance Officer under Curacao regulations, we use the term MLRO in our AML documentation for consistency and clarity.

The MLRO:

- Seniority and Autonomy: Has the necessary rank within the organisation and the independence to make decisions about AML/CFT matters without interference.
- Broad Expertise: Brings knowledge and experience from various jurisdictions as far as AML/CFT is concerned, ensuring an understanding of diverse regulations and practices.
- Clear Communication: Can convey AML/CFT topics effectively to all levels within the organisation.
- Continuous Learner: Regularly updates his knowledge on AML/CFT regulations and practices to keep the organization compliant.
- Proactive Approach: Keeps an eye on emerging AML/CFT threats and trends to ensure timely adaptation and response.

The MLRO is supported by the Fraud & AML Team ensuring the implementation of this policy on a day-to-day basis.

8.1.1 MLRO Core Functions

The MLRO is tasked with:

- Suspicious Activity Reports and Evaluation: Receiving, analyzing, and determining the validity of suspicious activity reports.
- Regulatory Reporting: Engaging with the relevant Financial Intelligence Unit (FIU) (or equivalent) about suspicious activities and cooperating in any subsequent investigations.

- Risk Management and Procedures: Evaluating risks and establishing preventative measures.
- Training and Education: Organising and implementing AML/CFT training programs.
- Appointing Designated Employees: Assigning roles in alignment with AML and CFT procedures.
- Reporting to the Board and Management: Delivering quarterly reports to the Board of Directors and Management.

8.1.2 MLRO Reports

Quarterly reports detailing AML/CFT activities are to be provided by the MLRO to the Board and Management. These reports serve as comprehensive reviews of the operator's compliance efforts.

8.1.3 Designated Employees

Understanding the significance of the MLRO's role, it's essential they remain available. However, to ensure continuity during unforeseen absences, entities may consider appointing a designated employee to stand in for the MLRO when required.

8.2 Fraud & AML Team

The Fraud & AML Team is essential in executing AML policies and procedures, focusing on monitoring and verifying medium/high-risk users and ensuring Enhanced Due Diligence (EDD) compliance. The team is also responsible for risk & fraud management, KYC document verification, and payout processing. Specific duties include:

- Operational Execution: Efficiently manage and execute payouts, monitor users daily, weekly, and monthly, and ensure adherence to AML policies and procedures.
- KYC & EDD Verification: Initiate KYC document requests for suspicious accounts, engage with customers for necessary documentation, and verify uploaded KYC documents.
- Monitoring & Reporting: Conduct regular reviews of user activities, report suspicious users to the MLRO, investigate customers using online resources and tools, and monitor medium/high-risk users.
- Fraud Detection: Identify and counteract fraudulent activities through various measures including account closures, investigations, and KYC document requests.

9. Training and Awareness

Training and awareness are crucial. While all employees receive basic awareness training, specific in-depth training targets teams directly involved in areas with potential AML risks. These teams are trained to recognize unusual customer behavior that may indicate money laundering, terrorism financing, or sanction evasion.

- **Recipients and Methodology:** In-depth training is provided to relevant teams and departments. Training is tailored to each employee's role, with key positions receiving face-to-face sessions delivered by both internal and external experts.
- **Frequency and Record Keeping:** Relevant teams receive initial training and annual refreshers. Training sessions, outcomes, and participant scores are documented, and records are kept for at least five years.

Content of AML/CFT Training

Training provides a comprehensive understanding of AML and CFT, with modules including:

- **Introduction to AML/CFT Concepts:** Overview of money laundering, terrorist financing, key laws, regulations, and the operator's obligations.
- **Vulnerabilities and Risks:** Understanding the operator's susceptibility to ML/TF, recognizing 'red flags', and understanding the consequences of non-compliance.
- **AML/CFT Policies and Procedures:** Overview of "Know Your Player" requirements, the operator's risk assessment protocols, reporting obligations, and the importance of not 'tipping off' suspects.
- **Identifying Unusual Activities:** Recognizing and understanding various 'red flags' and unusual activities that may indicate potential AML/CFT risks.

10. Money Laundering & Funding of Terrorism

10.1 Money Laundering

Money Laundering disguises proceeds from criminal activities, making them appear legitimate. This process typically involves three stages:

- **Placement:** Introducing criminal proceeds into circulation.
- **Layering:** Creating a complex series of transactions to distance funds from their origin.
- **Integration:** Merging the disguised funds into the legitimate economy.

Methods for money laundering in the iGaming sector include using prepaid cards, chip dumping, third-party transactions, structuring, dormant accounts, technological tools, using mules, and currency exchange.

The Licensed Company is committed to safeguarding the industry against these illicit activities and maintaining its integrity.

10.2 Funding of Terrorism

Funding of Terrorism provides resources, either directly or indirectly, to entities or individuals involved in terrorist activities. Terrorist financing involves collecting or providing funds for terrorist acts, irrespective of the source being legal or illegal.

In the iGaming environment, the risk of terrorist financing mainly arises during withdrawals. Indicators of potential terrorist financing risks include a customer's connection to high-risk regions or the use of anonymous payment methods.

10.3 Other Financial Crimes

Beyond money laundering and terrorist financing, numerous financial crimes are of concern, including:

- **Fraud:** Deceptive actions intending to secure an unfair or unlawful gain.
- **Theft:** Illegally appropriating another's property.
- **Tax-Related Crimes:** These range from tax evasion, where taxpayers intentionally underpay, to tax fraud and aggressive tax planning.
- **Bribery:** Influencing an individual in power by offering or receiving something of value.
- **False Accounting:** Manipulating financial information for deceptive purposes.

These crimes can serve as foundational offences to money laundering.

11. Reporting Obligations

As part of compliance measures, the operator enforces dual reporting responsibilities:

- **Internal Reporting Procedures:** Outlines steps for employees to report knowledge or suspicions of potential ML/TF activity.
- **External Reporting Procedures:** Details the protocol for MLRO (or a designated employee during the MLRO's absence) to inform the relevant authorities.

11.1 Internal Reporting Procedure

11.1.1 Obligations

Any officer, employee, or service provider to the Licensed Company must immediately report to the MLRO if they:

- Believe funds are associated with illicit activities or terrorist financing.
- Suspect an individual's involvement in ML/TF.
- Observe attempts to execute transactions linked to illicit funds or terrorist financing.

For external service providers, reports are initially directed to the Fraud & AML Team, which then escalates them to the MLRO or the designated employee.

11.1.2 Timing

Reports on potential ML/TF activity should be made urgently, ideally by the next working day. Transactions under suspicion should be halted pending guidance from the MLRO. If the MLRO is unavailable, the Designated Employee should be contacted.

11.1.3 Additional Internal Reports

Should employees observe further suspicious actions, additional reports to the MLRO or the Designated Employee are essential.

Confidentiality is paramount; not reporting is a violation, and no "tipping off" should occur.

11.1.4 MLRO Responsibilities

The MLRO should:

- Swiftly evaluate each internal report.
- Determine if a Suspicious Transaction Report (STR) is needed.
- Seek further information if required.

In decision-making, the MLRO must ensure:

- His role is determining potential ML/TF risks, not investigation.
- Prioritisation, especially in potential terrorist financing or significant ML cases.
- Quick access to all necessary information.
- Uninfluenced decisions, free from external pressures.
- Comprehensive documentation of all steps and decisions.

11.1.5 MLRO Conflicts of Interest

The MLRO must always act impartially. Conflicts of interest can arise due to the MLRO's personal or professional affiliations. If any officer or employee perceives a potential conflict or questions the MLRO's objectivity, they should direct their report to the Licensed Company's designated employee.

11.2 Definition of a Fact

A fact signifies a proven event or occurrence. It is an undeniable reality, grounded in evidence. In the context of an investigation, it can be specific details like the amount, date, time, or location of a transaction, or more intricate data like a player's financial trajectory.

11.3 Contextual Clarification

Context adds depth, offering insight into specific events, situations, or transactions. By juxtaposing a particular action or transaction against its broader context, it becomes easier to ascertain if it's suspicious or merely an anomaly.

11.4 Navigating Suspicion

Suspicion is a feeling that something isn't right. It might not have immediate evidence backing it but serves as a catalyst for further investigation.

11.4.1 Criteria for Reasonable Suspicion

For a Suspicious Transaction Report (STR) to be dispatched, there must exist 'reasonable grounds to suspect' a potential ML/TF event. The onus is not an absolute proof but a tangible basis.

11.4.2 Establishing Reasonable Grounds to Believe

A stronger criterion than suspicion. It suggests a higher likelihood, backed by substantial information, that a ML/TF event occurred.

11.5 Addressing Completed or Attempted Transactions

Whether a transaction is finalised or just attempted, any suspicions related to ML/TF must be reported.

11.6 Recognising Unusual Activities - Red Flags

Red flags act as cautionary markers suggesting possible irregularities which could be indicative of Money Laundering or Terrorist Financing activities. It is vital to approach these flags as indicators for further scrutiny rather than conclusive evidence. Here are some commonly recognized red flags:

- **Non-cooperation or reluctance:** Any unwillingness to cooperate with Customer Due Diligence (CDD) processes.
- **Misinformation:** Providing misleading, incorrect, or substantially false information.
- **Multiple account registrations:** An individual registering multiple accounts in a short timeframe.
- **Drastic transaction patterns:** Abrupt changes in deposit, withdrawal, or gaming habits.
- **Inconsistent behavior:** Deposit and withdrawal activities that aren't in line with the customer's known profile or income sources.
- **Negative associations:** Negative publicity or information linking a customer with criminal activities or affiliations.
- **Geographical concerns:** Transactions originating from or directed to regions known for elevated ML/TF risks or lacking adequate AML controls.
- **Anonymous payments:** Utilizing anonymous payment methods for account funding or withdrawals, such as certain types of prepaid cards.
- **Rapid movement of funds:** Depositing funds and quickly transferring them out without any apparent business reason.

By vigilantly monitoring for these red flags, the Licensed Company can ensure prompt identification and management of potential risks. Further investigation can then determine the legitimacy or suspicious nature of the observed activity.

11.7 Protocol for External Reporting

The MLRO, upon receiving an internal report, must quickly assess the situation. Depending on the analysis, the MLRO can choose to escalate it as an STR to the relevant FIU or keep a documented record of why it was not escalated. The utmost priority should be to uphold the integrity of the operator while ensuring compliance with regulatory standards.

In addition to submitting suspicious transaction reports to the FIU, the operator is committed to fulfilling all threshold-based AML reporting obligations as required by law, once the relevant reporting procedures have been fully established by the regulator and made available to all operators.11.9 Avoiding "Tipping Off"

"Tipping off" pertains to the unintentional or intentional revelation to a customer that they might be under investigation or suspicion for potential illicit activities. Such disclosure, at any phase, can endanger investigations and carries legal implications.

Main Tenets:

- **Confidentiality:** All information related to the identification of suspicious transactions or any subsequent report must be treated with strict confidentiality. Access to such knowledge should mainly be restricted to the MLRO and/or a designated representative.
- **Tactful Interactions:** Interactions with customers should be carried out judiciously, ensuring that no underlying suspicions are inadvertently disclosed. Routine inquiries should be posed discreetly without revealing any suspicions.
- **Restrictions on Disclosures:** After submitting an STR, this information must remain undisclosed to the customer or third parties. This confidentiality principle extends even within the corporate group, except when disclosure is legally mandated.
- **Anticipating and Managing Prejudice:** Consider potential repercussions on any FIU investigations before taking definitive actions. In situations of uncertainty, seeking guidance from the FIU can be beneficial.
- **Training and Communication:** Staff should undergo regular training and adhere to clear communication guidelines to prevent unintentional "tipping off."

The crux is that avoiding "tipping off" is essential for investigation integrity, while also protecting the organization and its personnel from legal repercussions.

11.10 Decision-making in Uncertain Circumstances

AML/CFT often presents situations steeped in ambiguity. Given the potential repercussions, a meticulous approach is paramount.

Guidelines:

- **Gather Comprehensive Information:** Accumulate all relevant data, exploring transaction histories, public databases, and consulting with colleagues when required.
- **Collaborative Decision-making:** Collaborating with senior management, the MLRO, or other relevant teams can often provide clarity in ambiguous situations.
- **Document Decisions:** Each decision and its underlying rationale should be meticulously recorded to provide clarity if later scrutinised.

- **Risk Evaluation:** Assess potential risks, including legal, reputational, financial, and operational, and proceed with caution when the risks seem high.
- **Stay Updated:** Remain informed about evolving AML/CFT regulations to ensure that decisions align with the latest guidelines.
- **Retrospective Analysis:** Reflect on past decisions to glean insights and lessons for future decisions.
- **Feedback Loop:** After a decision, especially in uncertain scenarios, obtain feedback from team members. Ensure that feedback mechanisms don't inadvertently breach "tipping off" principles by only sharing generalized information.
- **Uphold Integrity:** Prioritize the organization's integrity in all decisions. Even in ambiguity, act in the organization's and stakeholders' best interests.

To navigate AML/CFT uncertainties requires informed judgment, collaboration, and strict adherence to regulations. Regular training and fostering open yet discreet communication can enhance decision-making accuracy amidst ambiguity.

12. Customer's Data Collection & Processing

To meet legal obligations and support AML/CFT mandates, the Licensed Company retains comprehensive records of all business interactions with customers. Such records prove invaluable to entities like FIUs, supervisory bodies, and law enforcement agencies addressing potential ML/TF activities.

Key Areas of Data Collection:

- **Regulatory Reports:** All supporting documentation and draft reports are stored, with Suspicious Transaction Reports being retained for a minimum of five years post-creation.
- **Player Account Records:** These include photo identification, personal details, and financial data sourced from various channels.
- **Verification Documents:** This category includes Proof of ID, Proof of Address, Proof of Payment tailored to various payment methods, and Source of Wealth/Funds documentation, taking into account country-specific requirements.
- **Ongoing Monitoring Records:** Records of monitoring activities, such as established processes, acquired information, and actions related to high-risk players, are maintained.
- **PEP Information:** Data on persons determined as PEPs or their associates, including the position held, the source of their funds, and their wealth's origin, might be documented.

Retention Period:

Typically, records are preserved for at least five years, with possible extensions in specific scenarios by regulatory or law enforcement entities. After this retention period, a review for the necessity of continued data retention is conducted based on legal and data protection needs.

Data collection, processing and storing shall also be carried out in line with applicable law.

13. Risk-Based Approach (RBA)

The RBA plays a vital role in fortifying financial systems against potential misuse for ML/FT activities. With the understanding that ML/FT risks can differ widely, the RBA offers a framework for tailored risk responses.

Understanding and Implementing RBA:

- **Understanding Risks:** Thoroughly assess potential threats.
- **Varied Controls:** Adapt controls, policies, and procedures based on the identified risks.

Levels of Risk Assessment:

- **Business Risk Assessment:** Offers a comprehensive view of the business to evaluate its overall exposure to ML/FT.
- **Customer Risk Assessment:** Concentrates on individual transactions or relationships to measure associated risks.

Using the RBA, companies can deploy measures aligned with the level and nature of the identified risks, ensuring the optimal use of resources.

13.1 Business Risk Assessment (BRA)

The BRA serves as a guideline for the Licensed Company's team to evaluate the potential risks related to ML/FT in operations. This ongoing tool, periodically refined to reflect the evolving risk landscape, is a cornerstone of effective AML/CFT programs.

Shifts in the entities' technical solutions, sales strategies, or major external changes warrant a BRA review. At the very least, an annual review is customary.

If the BRA remains consistent post the annual review, the MLRO will notify the Board about its continued relevance.

13.2 Customer Risk Assessment (CRA)

The CRA is fundamental in identifying and addressing potential ML/TF risks individual customers might present to the company.

Based on the assessment, customers are segmented into risk categories: Low, Medium, or High Risk. The degree of risk associated with a customer dictates the thoroughness of the Customer Due Diligence (CDD) measures they undergo.

By implementing such categorizations, the entities ensure they are applying appropriate protective measures against potential ML/TF risks, making effective use of their resources, whilst adopting a risk-based approach.

The timing and methodology of customer risk assessments will be in accordance with applicable law.

13.3 CRA Methodology

Every player undergoes systematic assessment rooted in identified risk factors, aligning with the broader strategy to counteract ML/TF risks. Throughout their engagement with the platform, players are periodically evaluated. The cadence of these assessments correlates with the risk level ascribed to the account.

Risk determinants stem from player data, behavioral patterns, transactional histories, and associated investigative details. The aim of this risk scoring methodology is to offer a uniform system to evaluate ML/TF risk factors consistently across jurisdictions.

It is paramount to understand that designating a player as high-risk for ML/TF does not denote any illicit activity. Conversely, a low-risk label does not unequivocally certify a player's innocence. Hence, continuous vigilance and informed judgement in risk assessments are essential.

A bespoke Risk-Scoring Methodology is in place and undergoes annual reviews to ensure its continued relevance and efficacy, with any major modifications requiring Board and management endorsement before being rolled out.

13.4 Risk Appetite

This policy is aimed at providing the framework for the identification, assessment and mitigation of risk. A customer that is labeled as high-risk is only onboarded if they can furnish the necessary documents as specified in the Enhanced Due Diligence (EDD) protocols within the given timeline. Failure to comply grants the Licensed Company the authority to reject their application or service

request. This strategy ensures a harmonious balance between broad-reaching business practices and stringent regulatory adherence.

14. Politically Exposed Persons (PEP)

Politically Exposed Persons, often referred to as PEPs, are those who occupy, or have previously occupied, a prominent public function. Due to their elevated status, PEPs are more vulnerable to potential misuse in the context of corruption. Their significant influence could be misappropriated by ill-intentioned entities seeking to exploit them for money laundering or terrorist financing (ML/TF) schemes. Because of the inherent risks associated with PEPs, as well as their immediate family and close associates, instituting Enhanced Due Diligence (EDD) measures is essential.

PEPs, as outlined in the EU's AML Directives, are broadly categorized to account for potential risks they might present, irrespective of their national or international prominence. The directives include individuals who currently or formerly held significant public roles. It is further highlighted that the risk is not confined to the PEPs themselves; their family members and immediate acquaintances could also pose elevated risks due to their close connection to these influential individuals.

According to the EU Framework:

PEPs' family members typically comprise:

- The spouse or equivalent life partner
- Their offspring and their respective spouses or equivalent partners
- Their immediate ascendants.

PEPs' close associates include:

- Individuals known to have joint beneficial ownership or close business affiliations with the PEP
- Persons who possess sole beneficial ownership over entities or arrangements ostensibly established for the tangible benefit of the PEP.

AML screening checks and ongoing monitoring for politically exposed persons, sanctioned individuals, and adverse media will be conducted in accordance with applicable law.

15. Internal Control Rules

Within the organizational structure, the Fraud & AML team, together with the MLRO, are key components of the CX (Customer Experience) Department. Their collaboration ensures a cohesive approach in achieving shared goals.

Importantly, the CX Department's performance evaluation does not hinge on monetary or business-driven metrics. This detachment from financial considerations ensures unbiased assessments, reporting, and decision-making by its team members.

The mantle of oversight and quality assurance falls upon the MLRO and the Payments Operations & Fraud Manager. Their role encompasses ensuring consistent task execution and ongoing review of processes, guaranteeing alignment with established internal directives and procedures. To provide transparency and actionable insights, the MLRO submits a quarterly control report to the executive team, detailing compliance with the instituted rules and proposing potential modifications if deemed necessary.

The Legal Team provides oversight and acts as a second line of defence. The function of the Legal Counsel also supports in the effort to ensure compliance with relevant laws, regulations, and industry standards. They are crucial in ensuring that the Licensed Company meets its regulatory obligations and mitigate legal and reputational risks.

The second line of defence plays a critical role in enhancing the Licensed Company's overall risk management capabilities. The function provides oversight, guidance, and independent assessments to ensure that risks are identified, managed, and reported effectively, ultimately helping the Licensed Company achieve its strategic objectives while staying within the Licensed Company's acceptable risk tolerances and appetite.