Guidance

Institutional Risk Assessments

December 2024

Content

Introduction

These Guidelines are issued by the Financial Services Commission (the "FSC") as the supervisor of financial institutions (FIs) and the Financial Investigation Agency ("the FIA") as the Anti-Money Laundering, Counter-Financing of Terrorism and Counter-Proliferation Financing (AML/CFT/CPF) supervisor of Designated Non-Financial Businesses and Professions (DNFBPs) in the Virgin Islands (VI).

The FSC is responsible for the regulation and supervision of the financial services sector: (i) banking, (ii) insurance, (iii) trust and company services providers ("TSCPs"), (iv) investment business, (v) financing business (FB), (vi) money service businesses ("MSBs"), (vii) insolvency services, and (viii) virtual asset service providers ("VASPs"). The FIA is responsible for the supervision and monitoring of designated non-financial businesses and professions in the VI: (i) legal practitioners, (ii) notaries public, (iii) accountants, (iv) real estate agents, (vi) dealers in precious metals and stones ("DPMS"), (vii) high value goods dealers ("HVGD"), (viii) vehicle dealers, and (ix) persons engaged in the business of buying and selling boats. For the purposes of these Guidelines the entities, supervised by the FSC and FIA, are collectively referred to as "licensees".

As supervisors, the FSC and FIA are cognisant of the need to ensure all supervised entities are aware of the various risks related to their business. As members of the Council of Competent Authorities' Joint Supervisory Committee, the FSC and FIA are committed to ongoing cooperation and collaboration on matters that impact both FIs and DNFBPs, to ensure proper risk mitigation and enhance transparency, while maintaining the VI's reputation as a place to conduct legitimate and quality business.

These Guidelines have been developed for the benefit of assisting FIs and DNFBPs in the implementation of a risk-based approach for applying measures to mitigate ML, TF, and PF risks through proper and effective conduct of an institutional risk assessment (IRA).

Importantly, these Guidelines also buttress the provisions for compliance with the Anti-Money Laundering and Terrorist Financing Code of Practice (the "AMLTFCOP"), the Anti-Money Laundering Regulations ("AML Regulations"), the Regulatory Code (the "RC"), the Financial Investigation Agency Act (the "FIA Act") and the Financial Services Commission Act (the "FSC Act"), including any Explanatory Notes to these documents.

Comprehensive AML/CFT/CPF compliance by FIs and DNFBPs is essential to remaining up-to-date with evolving risks and threats that could adversely impact operations and compliance. These Guidelines also serve as a complement to the ongoing need to report and engage with the FSC, FIA and other Competent Authorities, including law enforcement agencies to achieve optimal results in preventing ML, TF and PF risks from being realised. These agencies include the Office of the Governor (GO), Attorney General's Chambers (AGC), Royal Virgin Islands Police Force (RVIPF) and the BVI International Tax Authority (ITA).

Background

The requirement to conduct an IRA applies to all FIs and DNFBPs that are subject to the AML Regulations and the supervisory regimes of the FSC and FIA. All licensees have obligations to comply with AML/CFT/CPF laws and regulations. These legal requirements are primarily derived from the international standards developed by the Financial Action Task Force (FATF) and are promulgated globally.

An IRA is an important element and tool of a Licensee's AML/CFT/CPF policies, procedures, systems and controls. Section 12 of the AMLTFCOP requires all relevant persons with AML/CFT/CPF obligations to conduct "an institutional money laundering, terrorist financing and proliferation financing risk assessment of its overall business." A licensee's IRA should clearly set out its compliance strategy and risk mitigation measures designed to minimise the ML, TF and PF risks to which a licensee may be exposed.

Why Carry out an Institutional Risk Assessment

Developing a comprehensive understanding of risk must include consideration of internal risks, risks inherent within the sector of operations, external risk factors such as cybersecurity risks and other international developments, as well as risks outlined in the National Risk Assessment (NRA) and other sectoral risk assessment reports. Such drivers impact a licensee's risk assessment framework. An IRA helps to aggregate these issues, while a risk-based approach allows licensees to allocate scarce resources to areas of heightened risks to mitigate against ML, TF, PF and other financial crimes.

An IRA is carried out in order to achieve the following:

- To determine the existence and extent of ML, TF and PF risks;
- To understand the risks to which the licensee is exposed;
- To help the licensee develop and implement controls to manage and mitigate risks identified;
- To help ensure full compliance with the legislation;
- To increase the focus on the products or services, transactions, customers, geographic locations and delivery channels that are more vulnerable to abuse by money launderers, terrorist financiers and other criminals;
- To ensure that the ML, TF and PF risks are assessed and mitigated before new products/services are offered; and
- To implement enhanced controls where higher risks are identified.

An IRA must be[1]:

- Documented and a record maintained of its approval process including formal approval by senior management and Board;
- Regularly reviewed and updated;
- Updated where risk inputs/factors change;
- Reviewed and updated on an ongoing basis but at least annually;
- Conducted prior to the launch or use of new products, business practices, delivery mechanisms and technological developments; and
- Be made available to the FSC or FIA when requested.

An IRA represents a comprehensive review and evaluation of the potential ML, TF and PF risks that may be faced by a licensee. Conducting an IRA provides a detailed document that identifies the range of risks impacting a licensee's operations. In drafting an IRA, licensees should be able to identify risks in a manner that allows them to drill down into various risk factors to provide qualitative information to ensure a robust risk assessment. By ensuring there is enough detail, compliance measures can be better targeted to mitigate against the identified risks. Importantly, licensees are required to update their IRA on a periodic basis given that risks, threats and typologies evolve.

Role of Board of Directors and/or Senior Management

The Board of Directors must review the licensee's IRA and approve the IRA, and any changes thereto.

The Board of Directors must also set out the licensee's Risk Tolerance Statement to clearly demarcate what risks are not acceptable, as well as the treatment of varying tiers of risk, as risks, once realised, can severely impact the licensee through financial loss and regulatory action.

Through the process of developing or updating an IRA, a licensee's Board of Directors is better positioned to make strategic decisions and improve operational efficiencies. Clearly defined risk management processes provides an operational environment with less ambiguity as to how to address the threats and vulnerabilities being faced by the licensee. An IRA also reduces or eliminates arbitrary and inconsistent responses to potential threats and vulnerabilities.

[1] Section 12 and accompanying Explanatory Notes of AMLTFCOP

[2] Board of Directors here also includes similar bodies for other types of legal persons and should be read in that regard as being applicable to all legal persons.

The danger in not conducting an IRA is that a licensee would be exposed to a variety of risks, without the necessary mechanisms to detect and prevent these risks. The Board of Directors has a fiduciary duty to ensure that a licensee has a comprehensive risk management and risk assessment framework that will enable the licensee to meet its strategic objectives and legal obligations.

Reference Material for Developing Institutional Risk Assessments

There are many factors that impact risk and the development of risk assessment frameworks for AML/CFT/CPF compliance. There are high-level documents that provide pertinent context to various risks faced by licensees. Such high-level documents include the FATF Recommendations and Methodology, as well as FATF or FSRB Typology Reports, other FATF or FSRB Sectorial Guidance Documents, and other relevant publications. Other relevant high-level documents have been developed domestically and include the comprehensive risk assessment reports produced by the VI[3] . The legal framework in which a licensee operates is also relevant in the development of a comprehensive IRA.

Risk Factors to be addressed in conducting Institutional Risk Assessment

The use of internal data is important for licensees to understand how to identify the parts of their business that are vulnerable to ML/TF/PF activity. For instance, a licensee may have identified a higher-risk jurisdiction, but without knowing how many clients it has emanating or operating from that jurisdiction or whether any of its products or services are used to facilitate business with that jurisdiction, this lack of data could result in a flawed assessment of risk.

This need for data requires that licensees have proper mechanisms to store and retrieve data and other information about their business, including data relating to their clients. It is important to understand that the IRA should, at first, examine the licensee's inherent risk, which is defined as the risk before the application of any control or mitigant.

The risk inputs required to develop a comprehensive IRA require there to be a framework to evaluate the inherent risks a licensee may be exposed to through its products, services, customer types, delivery channels, geography, new technologies, internal risks (which may be amalgamated as operational risks) and statutory compliance risks. Licensees must also be cognisant of their cybersecurity risks with the increased use of technological applications which may impact ML, TF or PF compliance by leaving the licensee's system vulnerable to abuse.

The information below is provided as a non-exhaustive guide to aid licensees in developing their IRAs. The information focuses on the types of data indicators that should be used and questions that could be asked to assess the following types of risk:

[3] Virgin Islands Money Laundering Risk Assessment 2022
Virgin Islands Proliferation Financing Risk Assessment 2022
Terrorist Financing Risk Assessment Report 2020
Money Laundering Risk Assessment Report 2020
Virgin Islands NRA Report 2016

- product, service and transaction risk
- customer risk
- country/geographic risk
- delivery channel risk

It also provides some practical examples of higher risk scenarios and typologies that should also be taken into account.

Product, Service and Transaction Risk

Data Indicators
• Types of products and services offered
• Volume of transactions executed
• Value and volume of assets, liabilities and transaction value, and other products and services, as applicable
• Suspicious transactions reports (STRs)
• National and Sectoral Risk Assessments (NRA/SRA) and other related studies/typologies provided/undertaken by relevant competent authorities and law enforcement agencies
Relevant Questions to Consider
• Does the product/service allow for anonymity?
• Does the product/service disguise or conceal the beneficial owner of your customer/ client?
• Does the product/service disguise or conceal the source of wealth (SoW) or source of funds (SoF) of your customer/ client (e.g. nominee type services)?
• Does the product/service allow for the movement of funds across borders?
• Does the product/service commonly involve receipt or payment in cash?
• Has the product/service been identified in any risk assessment produced by the VI and/or guidance material issued by VI competent authorities or law enforcement agencies as presenting a higher ML, TF or PF risk?
• Does the product/service allow for the acceptance of payment from third-parties or intermediaries?
• Does the product enable third parties who are not known to the institution to make use of it?
• To what extent is the usage of the product subject to parameters set by the licensee e.g., value limits, duration limits, transaction limits, etc.?
• To what extent is the usage of the product subject to penalties when certain conditions are not adhered to?
• Does the usage of the product entail structured transactions such as periodic payments at fixed intervals, or does it facilitate an unstructured flow of funds?
• Does the licensee understand the risks associated with new or innovative products or services, in particular, where this involves the use of new technologies or payment methods?
Examples of Higher Risk Scenarios and Typologies
• Products or services that allow client anonymity
• Products or services which can disguise and/or conceal beneficial ownership, SoF and SoW
• Where a customer is allowed to conduct business with higher risk business segments or to use the product/service on behalf of third parties
• Receipt and payment in high volume of cash
• Products that allow movement of funds swiftly and across borders including without clear economic reason
• Risk and situations identified in the NRA/SRA as presenting high risk

Customer Risk

Data Indicators
• Nature of SoF and SoW of customers
• Nature of business customers engage in
• Number of customers per risk category
• Number of customers involved in reports/negative information
• Number of clients from high-risk regions or jurisdictions
• Number of politically exposed persons
• Complexity of the client's corporate structures
Relevant Questions to Consider
• Is the customer a legal person or legal arrangement?
• Are there any complex ownership and control structures which may obscure the identity of beneficial ownership and controllers?
• Are any customers specified in the AMLTFCOP and AML Regulations as requiring ECDD?
• Do customers use complex business structures that offer no apparent financial benefits?
• Are customers politically exposed persons (PEP)?
• Are customers' business/transactions cash-intensive?
• Are customers involved in businesses associated with high levels of corruption?
• Do customers have an unexplained or difficult to verify SoW and/or SoF?
• Do customers conduct business through, or are they introduced by gatekeepers such as TCSPs, accountants, lawyers, or other professionals?
• Has a particular type or category of customer been identified in any National and/or Sectoral Risk Assessments (NRA/SRA) or other related studies/ typologies provided/undertaken by relevant competent authorities and law enforcement agencies as presenting a higher ML/TF risk?
Examples of Higher Risk Scenarios and Typologies
• Number of high risk customers and/or clients for each product/service assessed.
• Nature/category and number of customers involved in STRs. This heightened risk may indicate that the licensee is conducting business with higher risk clients.

Country/Geographic Risks[4]

Data Indicators
• Number of clients (and beneficial owners) from high risk countries
• Volume and value of transactions to and from high risk countries
• Licensees' beneficial owners, subsidiaries and other group entities in high risk countries
Higher risk countries are those that:
• Are known high risk to ML, TF or PF based on NRA, SRA or other typologies
• Are identified as high risk in ML, TF and PF risk assessments, external threat assessments, and other relevant risk assessments
• Have ineffective AML/CFT/CPF measures
• Have ineffective rule of law
• Have high levels of organised crime
• Have high levels of bribery and corruption
• Are a conflict zone or neighboring a TF conflict zone
• Are known for production and/or transnational shipment of illicit drugs
Relevant Questions to Consider
• Is the client domiciled in VI or in another country or does the client operate/do business in another country?
• Is the country subject to international sanctions, embargoes or similar measures issued by credible organisations such as the UNSC and the Financial Action Task Force (FATF)?
• Has the country been identified by credible organisations as lacking appropriate AML/CFT/CPF laws, regulations, and other measures?
• Has the country been identified by the FATF as having strategic AML/CFT/CPF deficiencies?
• Has the country been identified by credible sources as providing funding or support for terrorist activities or has designated terrorist organisations operating within it?
• Has the country been identified by credible sources as having significant levels of corruption, or as a source of narcotics, human trafficking and other criminal activities?
Examples of Higher Risk Scenarios and Typologies
• Consider regional and country risk. Identify high risk countries based on relevant sources such as NRAs, SRAs and other studies conducted by relevant government agencies, FATF list of high risk jurisdictions, FATF mutual evaluation reports, United Nations Office on Drugs and Crimes reports, and UNSC Resolutions.
• Licensee has branches or offices in identified high risk jurisdictions, or clients whose operations and/or transactions involve high risk jurisdictions.

[4] Licensees should bear in mind that significant exposure to higher risk regions or countries will elevate the risk related to geographic location. However, not all clients from a high-risk region or jurisdiction pose high risk. Licensees should understand how this will affect the clients' transactions and overall business activities.

Delivery Channel Risk

Data Indicators
• Available delivery channels
• Types and number of customers using the delivery channels
• Platforms posing higher risk based on NRAs, SRAs, and other relevant risk assessments, studies, or reports
Relevant Questions to Consider
• Does your business have non-face-to-face customers (via post, telephone, internet or via intermediaries)?
• Do you provide your products/services via the internet?
• Does your business have indirect relationships with customers (via intermediaries, third parties, etc.)?
• Do you provide your products/services via agents or intermediaries?
• Do you provide your products/services to overseas jurisdictions?
• Are prospective clients onboarded through direct interaction or through intermediaries/agents?
• Do clients transact business by engaging with the institution directly or through intermediaries/agents?
• Where clients interact through intermediaries/agents, are the intermediaries/agents subject to licensing and/or other regulatory requirements?
Examples of Higher Risk Scenarios and Typologies
• Possible indicators that may heighten risk for delivery channels include:
i. New technologies/new payment methods
ii. Non-face-to-face contact during onboarding
iii. Facilitation of cross-border transactions
iv. Use of intermediaries, agents, or third parties
• Determine the number of customers onboarded and/or who are using the channels with heightened ML, TF or PF risk

In addition, understanding the size and complexity of a licensee's business is important in determining how susceptible it is to ML, TF and PF. For example, a business that conducts complex cross-border transactions may be more susceptible to ML than one whose business is purely domestic. Similarly, businesses that are cash intensive are usually at more risk than those that rely on other verifiable payment methods. Licensees should also consider the extent to which their customers are able to use the services they provide to spread their funds across various products in order to avoid detection.

Assessing and Measuring Risk

A critical element of any institutional risk assessment framework is the risk identification process. Identifying the vulnerabilities to which a business may be exposed can provide clarity on the issues that can impact the licensee. These vulnerabilities should be subjected to a qualitative assessment to determine which are more likely to occur (probability) and those that can have a more significant impact on the licensee if they did occur (materiality). The information gathered in this process can be further developed into a matrix that outlines all these issues in a manner that is readily discernible.

		Materiality →				
		Negligible	Minor	Moderate	Significant	Severe
Probability ↑	Very Likely	Low-Med	Medium	Med-High	High	High
	Likely	Low	Low-Med	Medium	Med-High	High
	Possible	Low	Low-Med	Medium	Med-High	Med-High
	Unlikely	Low	Low-Med	Low-Med	Medium	Med-High
	Very Unlikely	Low	Low	Low-Med	Medium	Medium

The approach to conducting an IRA must be well documented and logically applied. This approach must encompass risk scoring various elements of each risk factor identified within a licensee's business, in order to achieve practical risk tiers. For example, customer risk will include several details of the customer, each of which could be risk scored in determining the risk rating or risk tier that a customer falls into. Licensees may opt for a minimum of three tiers of risk – Low, Medium and High – or elect for more granular risk tiers (for example, Low, Medium-Low, Medium-High and High). Applying a weighting to each risk factor should also be considered based on the informed judgment of the licensee on the relevance of the various risk factors. Weighting for each factor may vary based on the considered importance of the impact of the factor on the licensee's business.

When weighting risk factors, licensees must ensure that:

- weighting is not unduly influenced by just one factor;
- economic or profit considerations do not influence the weighting;
- weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- situations identified by national legislation, NRAs or SRAs as presenting a high ML, TF or PF risk are not allowed to be rated lower than in those assessments; and
- where an override mechanism is used to alter a generated score, the rationale for the decision to override the generated score is documented and approved at senior management and/or Board level.

Use of Technology in IRAs

Technological tools used for an IRA should be subject to testing to ensure that the results of risk assessments are in line with the documented approach. Licensees should be minded that the FSC or FIA should be able to assess the integrity of these technological tools. Technological tools help to digitally map threats and vulnerabilities that may occur within the licensee's operations. Well-built risk tools can aid a licensee in developing more nuanced approaches to risk. In some instances, licensees may also elect to calibrate their tools to generate dashboards that visually identify areas of greater risks, which should correlate to where resources are deployed. Technological tools used for an IRA should be subject to testing to ensure that the results of risk assessments are in line with the documented approach. Care should also be taken to reduce or eliminate false negative results that allow what should be a positive result to be incorrectly reflected.

Licensees should be minded that the FSC or FIA should be able to assess the integrity of these technological tools as part of their compliance monitoring processes.

Staff Training in Institutional Risk Assessments

Licensees should communicate the results of the IRA to employees, including senior management and the Board. Such training should include, amongst other things, the importance of risk management and strategies the licensee employs to implement the findings of the IRA in order to mitigate its risks. A record of such training should be properly maintained.

Outcomes of Institutional Risk Assessments: Risk Mitigation

Licensees must develop and implement policies and procedures to mitigate the ML, TF or PF risks they have identified through their IRA. The mitigation measures should include:

- Internal policies, procedures and controls nuanced to the risks identified that can fulfil obligations under the AMLTFCOP and AML Regulations;
- Adequate screening procedures to ensure high standards when hiring employees;
- Ongoing training for officers and employees to make them aware of the laws relating to ML, TF or PF;
- Policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value;
- Mechanisms for preventing ML, TF or PF, or any other serious offence;
- Independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with AML/CFT/CPF regime such as the AML Regulations and AMLTFCOP;
- Risk based approach to managing identified ML, TF or PF risks;

- Effective:
  - Customer identification procedures;
  - Record keeping and retention;
  - Reporting procedures;

- Confidentiality requirements and procedures;

- Transaction monitoring systems;

- Adequate screening procedures for customers against relevant sanctions lists; and

- Enhanced identification, verification and ongoing due diligence procedures with respect to customers who have been identified as high risk customers.

New Products, Services and Business Lines

Licensees are required to conduct risk assessments in relation to the development of new products, services and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Based on the inherent risk of new products/services, licensees should consider the functionalities/features of these products and services, target markets and customers using these products and services, among others. Some factors that may elevate risks include the presence of features that allow customer anonymity, disguised and/or concealed beneficial ownership and SoF and SoW of customers, large cash transactions, or movement of funds across borders. When considering risk licensees should consider any controls in place to mitigate the inherent risk of the new product or service. If the residual risk is high, the licensee should institute additional controls.

Additional controls may include, amongst other things:

- establishing transaction limits;

- requiring approval of higher authority such as senior management or the Board;

- conducting further due diligence on transactions that exceed thresholds; and

- providing the product only to certain/specific target market (e.g., low risk profile market).

Updating an Institutional Risk Assessment

Licensees should have in place systems and controls to keep their assessments of the ML, TF or PF risks associated with their business, and with their individual business relationships under review to ensure that their assessment of ML, TF or PF risks remains up-to-date and relevant. Licensees must ensure that changing, new or emerging risks can be captured in risk assessments and that resources allocated to mitigate identified risks remain proportionate to the risk level. Where a licensee is aware that a new risk has emerged, or an existing one has increased or decreased, this should be reflected in the IRA, as soon as possible.

New risks may include trigger events such as:

- the emergence of new technology;
- a new customer base;
- new services or products;
- entry into new geographic markets;
- new ML, TF or PF risks as identified by the FATF, CFATF, competent authorities or law enforcement agencies; or
- updated laws or regulations.

Additionally, where there has been an elevation in the level of risk identified, licensees should consider the risk management controls and the appropriateness of such to mitigate the elevated ML/TF/PF risks.

Issues such as internal suspicious transaction reports, compliance failures, findings from audit reports, and intelligence from staff, can also impact the IRA and thereby assist in updating risk assessments. Further, when updating risk assessments, licensees must always have regard to the identified threats and vulnerabilities from any MF, TF or PF risk assessments undergone by the VI or other relevant party on the VI, to ensure that ML, TF or PF risk inherent to the licensee is understood at the national/ country level and is reflected in the IRA.

Key Takeaways

Licensees should ensure that they identify, define and mitigate risks to which they are exposed. Standard Operating Procedures for the engagement of customers or provision of products and services offered by the licensee can aid in identifying points of potential exposure to risks. For example, licensees should ensure that their due diligence process for customers is complete and up-to-date prior to commencing business or delivering products or services for a new customer.

Identification of risk factors from the IRA aids Licensees in employing a risk-based approach to due diligence and implementing controls that are tailored to the specific risks presented in its customers, products or services.

Licensees should ensure that their IRA has clearly developed risk mitigation strategies for areas of heightened risks to ensure resources are deployed, and enhanced controls are developed for greatest positive effect. As risks continue to develop at a fast pace, licensees are guided to remain vigilant to emerging risks, threats and vulnerabilities.

Given the rate of change in risks, licensees should ideally conduct and/or review their IRAs on an annual basis. Identification of new threats, changes in regulation or changes in other material factors, could also trigger a review.

Finally, licensees should ensure that they review section 12 of the AMLTFCOP and the accompanying explanatory notes in their entity. The FSC and the FIA will be assessing compliance with the requirements of section 12 of the AMLTFCOP on an ongoing basis. To assist licensees in developing an effective IRA, Appendix 1 provides some helpful questions that licensees should ensure are addressed within their IRA or assessment of the effectiveness of their IRA.

Overarching Requirement for Compliance

Licensees must remain vigilant in relation to evolving ML, TF and PF threats, as well as other threats that can negatively impact their operations. To mitigate against these threats and resulting risks, licensees must be diligent in the application of AML/CFT/CPF measures. These measures must be holistic and integrate prudent governance and modern risk management strategies with a robust compliance framework. Licensees must remain agile and embed systems to allow for continual improvement in the efficiency and effectiveness of their AML/CFT/CPF compliance.

Table of Abbreviations and Acronyms

AML/CFT/CPF	Anti-Money Laundering, Countering Financing of Terrorism and Countering Proliferation Financing
AMLTFCOP	Anti-Money Laundering Terrorist Financing Code of Practice
AML Regulations	Anti-Money Laundering Regulations
DNFBPs	Designated Non-Financial Businesses and Professions
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FIA	Financial Investigation Agency
FIs	Financial Institutions
FSC	Financial Services Commission
FSRB	FATF Style Regional Body
IRA	Institutional Risk Assessment
Licensees	Financial Institutions and Designated Non-Financial Businesses and Professions
ML	Money Laundering
PEP	Politically Exposed Person
PF	Proliferation Financing
RAF	Risk Assessment Framework
RBA	Risk-Based Approach
SAR	Suspicious Activity Report
SoF	Source of Funds
SoW	Source of Wealth
STR	Suspicious Transaction Report
TF	Terrorism Financing
UNSC	United Nations Security Council

Appendix 1 - Institutional Risk Assessment - Helpful Considerations for Licensees

An Institutional Risk Assessment ("IRA") is an important element of a licensee's AML/CFT/CPF policies, procedures, systems and controls. The purpose of this Risk Assessment Checklist is to serve as a guide to objectively assessing a licensee's Risk Assessment Framework, and specifically, their IRA. The IRA of a licensee should clearly set out the AML/CFT/CPF compliance strategy and risk mitigation measures designed to decrease and eliminate the risks of possible money laundering, terrorist financing or proliferation financing.

Question	Yes	No
GOVERNANCE & RISK ASSESSMENT FRAMEWORK Does the licensee's Institutional Risk Assessment Framework cover the following:		
A. Board Review & Establishment of Risk Framework		
1. Is there a Board approved Risk Assessment Framework (which may include a Risk Tolerance Statement)?		
2. Does the Risk Assessment Framework cover the vulnerabilities that could be presented from customers, geography, products and/or services and delivery channels?		
3. Has the Board reviewed and/or updated the Risk Assessment Framework within the past year?		
4. Have any updates made to the Licensee's Risk Assessment Framework (in part or in whole) reflected updates to the Virgin Islands' AML/CFT/CPF regime?		
5. Has the Licensee's Risk Assessment Framework been informed by relevant risk assessment reports produced and published by the Virgin Islands (listed below) or any other domestic, regional or international agency, competent authority or law enforcement agency on the risk emanating in or from within VI? a) Virgin Islands National Risk Assessment Report, 2016 b) Money Laundering Risk Assessment Report, 2020 c) Terrorist Financing Risk Assessment Report, 2020 d) Virgin Islands Proliferation Financing Risk Assessment, 2022 e) Virgin Islands Money Laundering Risk Assessment, 2022		
6. Has the Risk Assessment Framework been informed by relevant sectoral FATF Typologies Report?		
7. Are there records of the Board's decisions regarding the entity's risk assessment framework, including reports and resolutions easily accessible to evidence strategic decision-making?		
8. Has the Risk Assessment Framework been informed by any other risk factor documented and cited from a source not set out in the above (for example, Wolfsberg Group, IOSCO, IAIS, BCBS, GIFCS)?		
9. Are the resources used to aid in the assessment of risks reviewed on an annual basis by the MLRO/ Compliance Officer? If yes, are the results of this assessment reported to the Board?		
10. Where the entity deviates from the approved application of risk scoring, is the rationale for the deviation set out in a clear and logical manner?		
11. Does the risk assessment framework set out clear risk mitigation measures in relation to all facets of risks as outlined below?		

Question	Yes	No
i. Client/Customer		
ii. Country/Geographic		
iii. Product		
iv. Service		
v. Delivery Channel		
vi. Transaction Risk including One-off Transactions		
vii. Other Qualitative Risk[5]		
12. Does the Licensee's risk mitigation measures include provisions to reduce or eliminate data corruption or data theft?		
13. Does the Licensee's risk mitigation measures include provisions to reduce or eliminate the threat of cybersecurity breaches?		
B. Implementation of Institutional Risk Systems & Controls		
14. Is there a logical Risk Scoring or Risk Rating System in use by the Licensee?		
15. Does the Licensee's risk rating methodology support the Licensee's Risk Tolerance Statement?		
16. Does the Licensee's rating system provide for appropriate risk categories (i.e [Low, Medium, High] or [Low, Medium Low, Medium, Medium High, High])?		
17. Is the Licensee's senior management sign-off required for the taking on of high-risk business and for the provision of a high-risk product/service?		
18. Is the Licensee's senior management required to annually sign off on the retention of high-risk business?		
19. Does the Licensee appropriately apply risk ratings for all clients?		
20. Does the Licensee appropriately apply risk ratings for all beneficial owners?		
21. Are there clear policies, procedures, indicators and monitoring provisions to identify shifts in risks (that would trigger a reassessment of risks where risks have increased or decreased)?		
22. Does the risk assessment include an assessment of country/geographic risk in relation to countries that impact all aspects of the Licensee's business?		
23. Does the Licensee rely on third parties for the introduction of clients?		
24. Where the Licensee relies on third parties for the introduction of clients, is that reliance material to its business?		
25. Does the risk assessment include an assessment of engagement with third parties upon whom the entity relies on for introduction of clients?		
26. Where the Licensee's business relies on third parties for the introduction of clients, has testing been carried out within 12 months to assess and verify the ultimate beneficial ownership, directors and senior officers?		
27. Where the Licensee's business relies on third parties for the introduction of clients, has screening of beneficial owners been carried out within 12 months to ensure compliance with sanctions?		

[5] Additional risk factors that can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML/CFT controls. Qualitative risk factors that directly or indirectly affect inherent risk factors may include:
• Significant strategy and operational changes;
• Structure of ownership/ business e.g., presence of subsidiaries; and
• National Risk Assessments.

Question	Yes	No
28. Does the risk assessment include an assessment of each product offered by the Licensee including new ones?		
29. Does the risk assessment include an assessment of each service offered by the Licensee including new ones?		
30. Does the risk assessment include an assessment of bundled products and/or services offered by the entity?		
31. Does the risk assessment include an assessment of the manner in which the entity delivers its products and/or services?		
32. Does the risk assessment include an assessment of cyber and other technological resiliency? Is this being conducted on a periodic basis (monthly, quarterly or annually)?		
33. Is there a Business Continuity Plan in place that addresses material risks and been tested?		
34. Does the risk assessment include an assessment of vendors to whom the entity's activities are outsourced?		
C. Effectiveness - Institutional Risk Assessment Process		
35. Is there evidence that the Licensee applies risk assessment measures consistently in relation to its customers?		
36. Is there evidence that the Licensee consistently applies risk assessment measures for one-off transactions?		
37. Is there evidence that the Licensee consistently applies risk assessment measures in relation to reliance on third parties where business has been introduced?		
38. Are there documented steps for staff to take where risks are unclear?		
39. Is there evidence that the Licensee has assessed its threats and vulnerabilities that could result in money laundering, terrorist financing, proliferation financing and other financial crimes?		
40. Has the Licensee's assessment of its threats and vulnerabilities include reviews of relevant Virgin Islands National Risk Assessment Reports and FATF Risk-based Sectoral Guidance Reports?		
41. Has the Licensee documented a resource contingency plan/strategy to address 'key person risks' from materialising (where an individual's absence can materially impact the Licensee's ability to operate normally)?		
42. Does the risk assessment include an assessment of the manner in which the entity delivers its products and/or services?		
43. Does the risk assessment include an assessment of geographical exposure of the risk subject (i.e., client, third party, service, delivery channel, etc.)?		
44. Are the resources used to aid in the assessment of risks reviewed on an annual basis by the Compliance Officer, MLRO or Risk Officer?		
45. Does the MLRO, Compliance Team or Internal Audit conduct spot checks (or scoped internal audits) on the application of risk assessment?		
46. Was a check conducted within the last 12 months?		
47. Have the results of this assessment been reported to the Board of Directors?		
48. Has the Board of Directors provided direction on any additional action? If so, the action and the deadline by which completion was required should be documented?		
49. Is there a documented methodology (approved by the Board) to assess the risks of new products and/or services?		
50. Are there risk mitigation measures in place to prevent internal ML, TF and PF risks/threats from occurring?		