Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue, Manila

BAGONG PILIPINAS

Circular Letter No.	2024-16
Date	21 August 2024

CIRCULAR LETTER

TO : **ALL INSURANCE/REINSURANCE COMPANIES, MUTUAL BENEFIT ASSOCIATIONS, INSURANCE AND REINSURANCE BROKERS, PRE-NEED COMPANIES AND HEALTH MAINTENANCE ORGANIZATIONS**

SUBJECT : **GUIDELINES FOR THE CONDUCT OF INSTITUTIONAL RISK ASSESSMENT (IRA)**

WHEREAS, IC Circular Letter 2018-48, as amended, requires the conduct of institutional risk assessments at least once every two (2) years, or as often as the Board or senior management may direct, depending on the level of risks identified in the previous assessment or other relevant AML/CFT developments that may have an impact on the ICRE's operations;

WHEREAS, the Insurance Commission, as Supervising Authority, is mandated to assist the Anti-Money Laundering Council (AMLC) in supervising the implementation of the Anti-Money Laundering Act (AMLA), as amended, and the Terrorist Financing Prevention and Suppression Act (TFPSA), and their respective Implementing Rules and Regulations (IRRs), and other AMLC issuances;

WHEREAS, to be able to focus supervisory efforts and allocate resources where the risks of money laundering (ML), terrorist financing (TF), and proliferation financing (PF) are higher, it is necessary to identify, assess, and understand the ML/TF and PF risks to which the regulated entities supervised by this Commission are exposed so that IC can have more impact at the tactical level to assess the ML/TF risks per sector, and define the scope and depth of its inspection;

Head Office, P.O. Box 3589 Manila | Trunkline: +(632)8523-8461 | Fax. No: +(632)8522-1434 | www.insurance.gov.ph

WHEREAS, a risk-based strategy for anti-money laundering and combating the financing of terrorism (AML/CFT) and proliferation financing (PF) will ensure that appropriate measures commensurate with those risks are adopted to mitigate them effectively;

WHEREAS, institutional risk assessment is the foundation of a proportionate risk-based AML/CFT framework on which the ICREs AML/CFT compliance program is based;

WHEREAS, Rule 15, Chapter V of the 2018 IRR of the AMLA, likewise requires covered persons to take adequate actions to identify, assess, and understand the ML, TF, and PF risks by performing their institutional risk assessment as well as formulating and implementing their risk management;

NOW, THEREFORE, this Commission issues this guideline to ensure that the AML/CFT institutional risk assessment by all IC Regulated Entities is conducted comprehensively and uniformly.

For your strict compliance.

REYNALDO A. REGALADO
Insurance Commissioner

INSURANCE COMMISSION

GUIDELINES FOR THE CONDUCT OF

INSTITUTIONAL RISK ASSESSMENT

2024

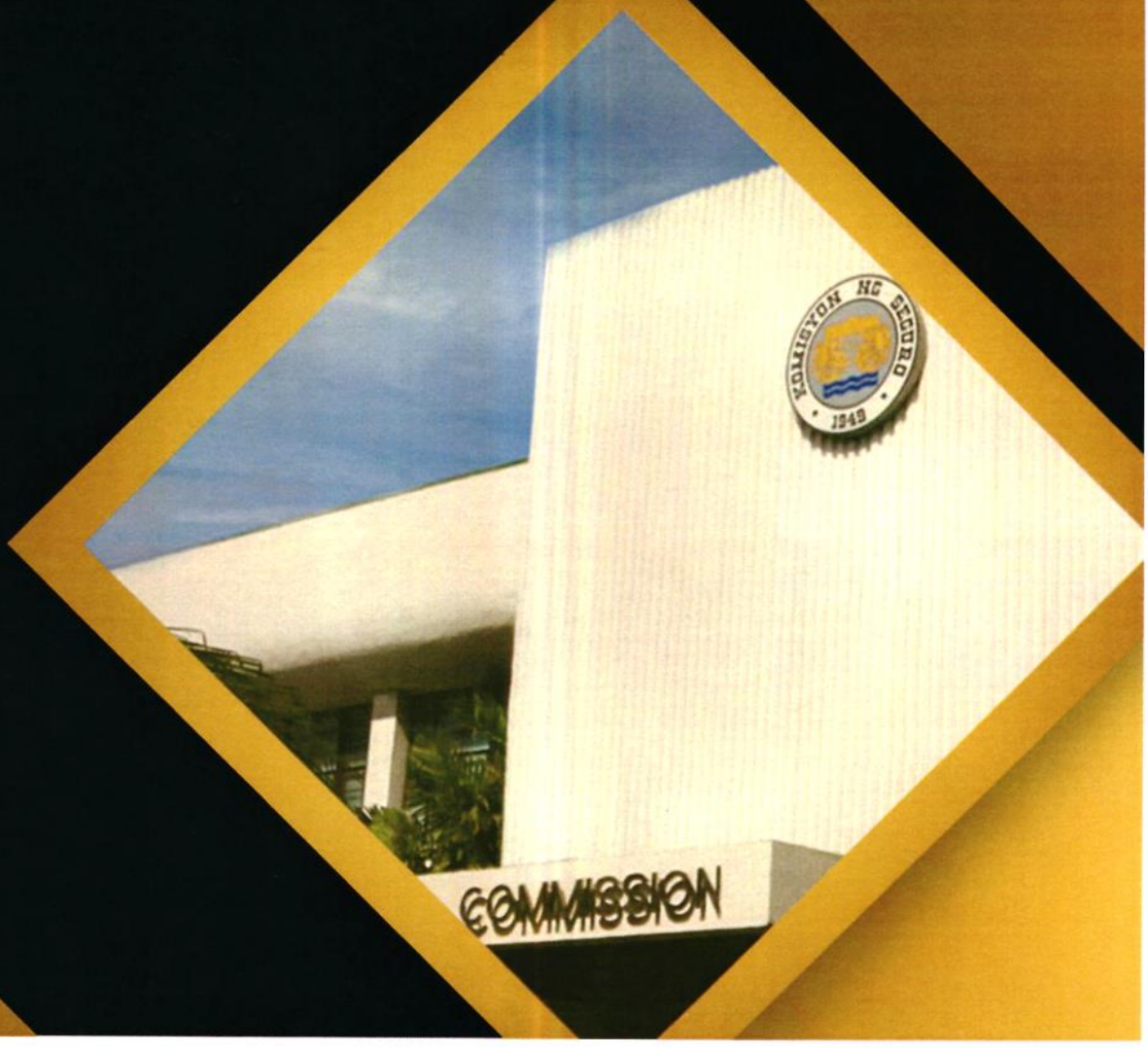


TABLE OF CONTENTS

TITLE I

INTRODUCTION

The Institutional Risk Assessment (IRA) forms the basis of a balanced risk-based framework aimed at combating money laundering (ML), terrorist financing (TF), proliferation financing (PF), and mitigating sanctions risks. This IRA employs a methodical approach to identify, analyze, and comprehend the risks associated with ML/TF/PF. The results of the IRA are crucial in shaping and enhancing AML/CTPF policies, systems, controls, and procedures, ensuring they align with the operations and risk profiles of ICREs.

This document outlines the regulatory obligations and offers practical insights to assist ICREs in conducting effective IRAs. It integrates current regulations, international standards, and industry best practices, providing a flexible framework adaptable to the diverse activities and operational complexities of ICREs, regardless of their business models.

TITLE II

GOVERNING REGULATIONS AND INTERNATIONAL STANDARDS

Key regulations and international standards on IRA include:

1. Rule 15, Section 1 (Institutional Risk Assessment) of the Implementing Rules and Regulations (IRRs) of the Anti-Money Laundering Act (AMLA) of 2001, as amended – provides that covered persons shall take appropriate steps to identify, assess, and understand their ML/TF risks.

2. Section 2(a) of Insurance Commission (IC) Circular Letter (CL) No. 2019-65 dated 22 November 2019 provides that ICREs shall take appropriate steps to identify, assess, and understand its AML/CTF risks in relation to its customers, its business, products and services, geographical exposures, transactions, delivery channels, and size, among others; and appropriately define and document its risk-based approach. The risk assessment shall include both quantitative and qualitative factors.

3. Financial Action Task Force (FATF) Recommendation 1 requires countries and financial institutions to identify, assess, and understand ML and TF risks they face and take appropriate action.

4. FATF Recommendation 6 requires the implementation of TFS regimes to comply with the United Nations Security Council (UNSC) resolutions relating to the prevention and suppression of terrorism and terrorism financing (TF).

5. FATF Recommendation 7 necessitates the implementation of Targeted Financial Sanctions (TFS) to comply with the UNSC resolutions relating to the prevention, suppression, and disruption of the proliferation of weapons of mass destruction and its financing.

6. Republic Act (RA) 10168 or the TF Prevention and Suppression Act of 2021, RA 11479 or the Anti-Terrorism Act of 2020, RA 9160 or the AMLA, as amended, and their IRRs on provisions relating to the implementation of TFS.

TITLE III

OBJECTIVES OF THE IRA

The institutional risk assessment of ICREs involves defining the methodologies for AML/CFT and TFS risk assessments, specifying scope, and considering key elements to determine residual risk. It identifies sources of ML/TF/PF and sanctions risks, assesses vulnerabilities in business operations, and evaluates existing controls.

Following the assessment of residual risk, action plans are devised.

ICREs are required to develop tailored policies, controls, and procedures to effectively manage and mitigate identified risks, thereby implementing a risk-focused strategy against ML, TF, and PF. The IRA should describe what AML/CFT and Targeted Financial Sanction Risk Assessments entail, the scope, and the elements considered to arrive at the residual risk.

This approach results in a risk-driven strategy for preventing and mitigating ML, TF, and PF. The results of the IRA are particularly valuable as they provide key insights into various aspects of risk management:

1. Present to the Board of Directors (BOD) and Senior Management information on the ICRE's ML/TF/PF and sanctions risks landscape as well as AML/CTPF control gaps and opportunities for improvements. It supports the alignment of the residual risk with the set risk appetite of the ICRE;

2. Inform remediation strategies and development or enhancements of AML/CTPF policies, systems, controls, processes, and procedures, as articulated in the ML/TF/PF Prevention Program (MTPP);

3. Direct focus on issues and concerns that present higher risks such that where higher risks are identified, enhanced measures should be taken to manage and mitigate the risks; and

4. Enable ICREs to deploy reduced preventive measures to those proven identified low-risk areas to ensure that unwarranted burdens or requirements are not imposed on lower-risk clients, products, and services.

TITLE IV

REGULATORY EXPECTATIONS ON IRA

ICREs shall be guided by the relevant regulatory expectations such as:

1. The IRA shall (a) use a methodology that is suited to the ICRE's risk and context and considers all relevant risk factors, such as customers, countries or geographic areas of operations, products, services, transactions, or delivery channels, including information from the results of the national and sectoral risk assessments (NRA/SRA); (b) adequately document its results and findings; and (c) provide up-to-date assessments.

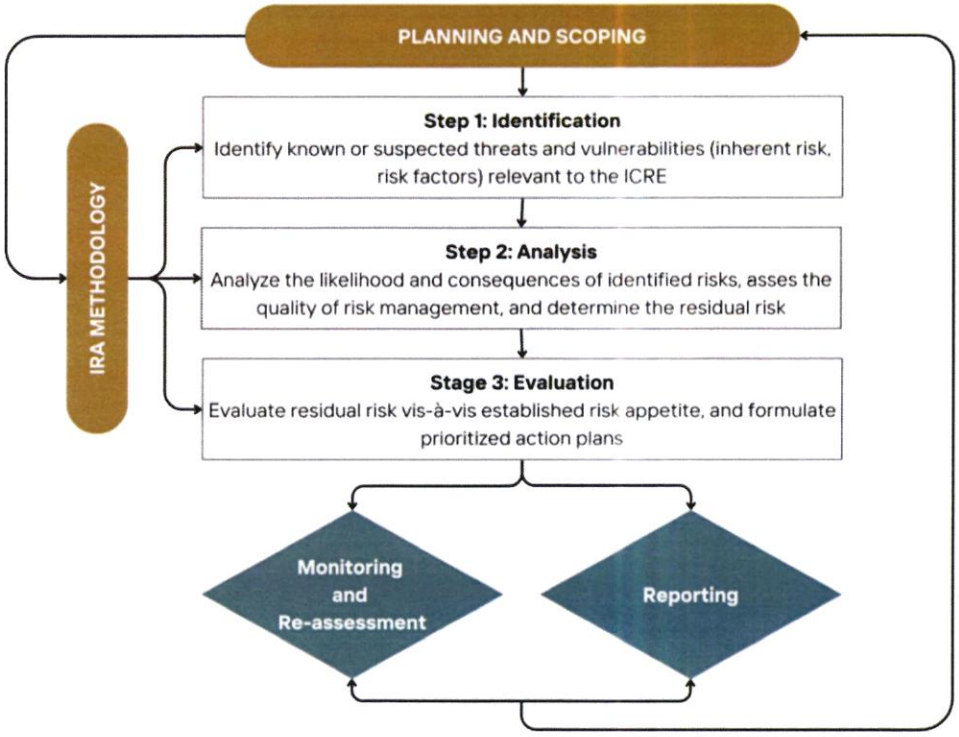
2. ICREs must identify and assess the risks related to ML/TF/PF, as well as sanctions risks, that may emerge in connection with creating or implementing new products/services, business practices, delivery channels, and technologies. This risk assessment should be an essential part of the process of developing a product or service, and it should be conducted before the launch of new products, business practices, or the adoption of new or emerging technologies.

3. Based on the findings from the risk assessments for IRA and/or new products or business practices, ICREs should implement suitable actions to control and reduce the ML/TF/PF and sanctions risks identified. This includes implementing additional measures for areas categorized as high-risk, which should be clearly outlined in the MTPP.

4. The risk assessment must be accessible to the IC for examination purposes or when needed for risk-based supervision.

Process diagram:

IRA PROCESS



Note: Based on FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment, February 2013.

DEFINITION OF TERMS

1. **Risk-Based Approach -** the identification, assessment, and understanding of the ML,TF, and PF risks to which an insurer is exposed and implementing measures commensurate with the identified risks to effectively mitigate them.

   It allows an insurer to apply appropriate policies, procedures, systems, and controls to manage and mitigate the ML, TF, and PF risks based on the nature, scale, and complexity of the entity's business and ML, TF, and PF risk profile.

   It also facilitates the effective allocation of resources to manage and mitigate the identified ML, TF, and PF risks.

2. **ML/TF Risks consist of:**

   a. **Threat-** persons or groups of people, objects, or activity with the potential to cause harm. In ML, TF, and PF contexts, a threat could be criminals, facilitators or transactors, beneficial owners, their funds, or even terrorist groups.
   b. **Vulnerability –** elements of a business that the threat may exploit or that may support or facilitate its activities. In ML, TF, and PF contexts, vulnerabilities could be weak controls within a reporting entity, offering high-risk products or services, etc.; and
   c. **Consequence –** refers to the impact or harm that ML, TF, and PF may cause, such as the impact on reputation and imposition of regulatory sanctions.

3. **Inherent Risk –** the intrinsic risk of an event or circumstance that exists before the application of controls or mitigation measures.

4. **Risk Management –** the process that includes the recognition of ML, TF, and PF risks, the assessment of these risks, and the development of methods to manage and mitigate the risks that have been identified.

5. **Risk factors** - specific threats or vulnerabilities that are the causes, sources, or drivers of ML/TF/PF risks.

6. **Residual Risks** – the level of risk that remains after the implementation of mitigation measures and controls.

1. PLANNING AND SCOPING

A systematic process is important to a meaningful ML/TF/PF and sanctions risk assessment. ICREs may consider the following planning and scoping activities to facilitate the successful conduct of the IRA:

a. Define the objectives and scope of the assessment.

   Objective. There must be clarity at the onset about the purpose or goal of the assessment. The thrust of the assessment should be aimed at identifying the sources of ML/TF/PF risks and vulnerabilities to enable the development of necessary measures to mitigate or reduce an assessed level of risk to a lower or acceptable level in line with the defined risk appetite.

   Scope. It sets the ambit, coverage, or extent, as well as the covered period of the IRA. ICREs also need to define the focus of the IRA, whether it is conducting a combined or separate assessment for ML/TF/PF and sanctions risks.

b. Prepare a project plan, identify the units and personnel who will be involved in the IRA, and establish milestones and timelines.

   The IRA should have the strong support of the BOD and Senior Management. A clear project plan describing the process and the roles and responsibilities of those involved in the IRA process is critical. Relevant and key units involved in the conduct of the IRA should be identified, including designating a champion that will ensure the completion of the IRA. Business lines (e.g., branches and head office units), or those units with ML/TF/PF risk exposures should actively participate and contribute to the assessment process. Key milestones and timelines for the completion of the IRA should be defined.

Figure 1. IRA Team

> In one ICRE, the Compliance Office leads the conduct of the IRA, supported by the BOD, senior officers, and heads of relevant business units such as New Business Units, Underwriting, Policy and Customer Service Department (for after-sales), Claims Department, Database Admin-Digital and Technological Services, Internal Audit, and Risk Management.

c. Devise a feasible mechanism for data collection, analysis, and updating.

The value of the results of the IRA will be shaped by the extent and quality of data and information used. Relevant quantitative and qualitative data or information must be considered in the IRA process, such as results of the national, sectoral, and other relevant risk assessments conducted by the Anti-Money Laundering Council (AMLC), the IC, or other applicable regulatory authorities, as well as relevant typology studies conducted by international organizations (e.g., FATF and Asia Pacific Group on Money Laundering [APG]). ICRES should develop an appropriate data collection process or mechanism to record and facilitate continuous gathering and/or updating of data and information needed for the conduct of the IRA. The results should be adequately documented, including the basis thereof.

Figure 2. Survey Questionnaire

An ICRE prepared a customized questionnaire to systematically capture data and information from different business units. This includes specific questions related to the inherent vulnerability of the products/services offered, as well as controls implemented.

2. IRA METHODOLOGY

When conducting an IRA, it is crucial to select an appropriate methodology. There is no one-size-fits-all approach when it comes to assessing ML/TF/PF and sanctions risks. The risk assessment methodology should be tailored to the nature and complexity of the ICRE's activities and operations. For instance, more complex ICREs should utilize a detailed or sophisticated assessment process, while smaller or less complex ICREs may opt for a simpler methodology. The key is to choose a methodology that effectively captures and analyzes the ICRE's actual risk profile and achieves the defined objectives of the assessment.

Figure 3. Risk Assessment Methodology

An ICRE uses a risk assessment methodology that measures ML/TF/PF risks based on threat, vulnerability, and consequences. The ICRE assessed each risk factor, such as ML threat related to web-related crimes and TF, the likelihood that it may happen by considering both the inherent and control risk (vulnerability assessment) and the impact (consequence assessment) of each risk to the ICRE.

3. THREE STAGES OF THE RISK ASSESSMENT PROCESS

STAGE 1: RISK IDENTIFICATION

This entails the identification of the various ML/TF/PF threats and vulnerabilities (inherent risks) germane to the ICRE's business operations.

a. Identifying ML/TF/PF Threat

It is important to have a clear understanding of potential threats by identifying relevant predicate offenses and their proceeds, as well as gathering information related to known or suspected threats and sectors, products, or services that may be exploited. When identifying threats, ICREs may refer to various sources such as:

a) Results of the NRA/SRA, which usually provides information on the money laundering/terrorist financing proceeds of the crime threat environment and the financial services used in the proceeds of illegal activities.

b) Analysis of suspicious transaction reports (STRs), filed fraud cases, freeze orders, inquiries, and asset preservation orders received.

c) News articles, reliable reports, and published studies on ML/TF/PF, proceeds of crime, and sanctions typologies.

Figure 4. Sample Threat Guide Questions

- Is ICRE exposed to proceeds of crimes such as drug trafficking, smuggling, fraud, and online sexual exploitation of children (OSEC), among others?
- Were there actual crimes in which the ICRE was involved, and what is its exposure?
- Is the ICRE exposed to the threat of terrorism, TF, and PF, and what is the extent of such exposure?

Figure 5. Sample Risk Scenario of an ICRE

An ICRE identified its "Risk Scenario" in terms of crimes that can be committed (e.g., web-related crimes, OSEC, and TF), and the types of customers/transactions that can facilitate ML/TF/PF-related activities (e.g., transactions outside of the normal behavior or financial profile of the customer, and unusual cross-border transactions).

Key risk scenarios were identified based on global and local risks as contained in relevant risk assessments (e.g., SRA, NRA, news, or general insurance, pre-need, and HMO experience).

Sanctions risk, which can be defined as the risk of losses arising from failure to implement relevant sanctions requirements, including TFS, should also be assessed. In relation to this, TFS risk assessment refers to the analysis of risks of potential breach, non-compliance, non-implementation, or evasion of TFS obligations (e.g., designated individuals and entities were able to access financial services due to weak customer onboarding procedures and/or lack of staff training[1]) and taking appropriate mitigating measures commensurate with the level of identified risks[2].

TFS involves freezing assets and imposing prohibitions to ensure that funds or other assets[3] are not made available, directly or indirectly, to benefit designated individuals and entities. It's important to note that TFS implementation is based on specific rules that must be fully adhered to. However, carrying out a risk assessment for TFS helps in identifying risk-based actions that ICREs should take to strengthen and complement the complete implementation of TFS requirements.

b. Identifying ML/TF/PF Vulnerabilities

ML/TF/PF risk exists when ML/TF/PF threats exploit related vulnerabilities, including inherent risk.

ML/TF/PF Inherent Risk

The concept of inherent risk pertains to the inherent level of ML/TF/PF and sanctions risks associated with an ICRE's business and relationships before any controls or preventive measures are put in place. The inherent risk in the business is influenced by various factors such as the nature, scale, features, and complexity of the products or services offered, delivery channels, geographical location of the ICRE's operations, as well as any new developments and technologies adopted in the operations. In the context of relationship-based risk assessment, the focus is on the customers and the ICRE's business relationships with them, considering factors such as the products, services, and delivery channels used by the customers, their geographic location, their transactions, technological advancements available to them, and the historical patterns of their transactions.

To identify inherent risks effectively, ICREs should use their adopted methodology. This involves gathering data and information to evaluate key factors such as the nature, scale, diversity, and geographic scope of the business, target market, customer profiles, as well

[1] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-AssessmentMitigation.pdf

[2] https://www.fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing2020.html

[3] 2021 AMLC Sanctions Guidelines, Chapter 1

as the value and volume of transactions. Annex A offers a practical example of data and information that can aid in identifying inherent risks. Establishing a scoring system for each inherent risk factor, supported by appropriate parameters, thresholds, and assumptions, is beneficial for the rating process. This scoring system should be customized to align with the size and nature of the ICRE's business operations. For an illustration, Annex B provides sample parameters for risk classifications.

The Inherent Risk Scoring will help determine the overall level of ML/TF/PF risk and will also provide an assessment of the specific factors contributing significantly to the inherent risk. For instance, the vulnerability of an ICRE to ML threats related to online sexual exploitation of children Sex (OSEC) can be evaluated by assessing the inherent risk of its remittance product, the types of clients it deals with, and geographical risk, such as the volume and value of transactions to and from countries associated with OSEC, as well as the extent of clients potentially involved in OSEC-related criminal activities. Detailed examples of inherent risk scoring and assessment matrices can be found in Figures 6 and 7.

Figure 6: Example of Inherent Risk Scoring

An ICRE adopts a risk scoring that considers inherent risk factors with equivalent risk points for each of the criteria and an overall risk score equivalent to each risk classification. The risk scoring is calibrated periodically to ensure adequacy and reliability of input data and results.

Low	Moderate	Above Average	High
0-30	31-60	61-90	91-120

Figure 7. Example of Inherent Risk Assessment

Rating	Description
High	Excessive level of inherent risk
Above Average	Significant level of inherent risk
Moderate	Manageable level of risk
Low	Marginal level of inherent risk

TFS Inherent Risk

In the identification of inherent risk related to TFS, ICREs should consider the TF/PF risk context as well as the following:

i. Relevant sanctions lists. Sanctions risk exposure to domestically designated personalities and those in the UNSC resolutions on TF and PF. TFS requirements are rules-based, which means full application of TFS. Meanwhile, ICREs may adopt other sanctions lists such as the European Union and Office of Foreign Assets Control lists, depending on their business operations and risk profile.
ii. Products, services, channels, and/or transactions that are exposed to TFS risks. These may include trade finance and wire transfers, among others, due to their cross-border element.
iii. Exposure to sanctioned countries or those that are known to be involved or cater to the sanctioned individuals and entities, or jurisdictions/domestic regions with a high prevalence of terrorism, TF, and PF-related activities. This can be sourced from relevant reports such as NRA/SRA, regional risk assessment (or Enterprise Wide Risk Assessment [EWRA]), and other studies conducted by the relevant agencies (e.g., Anti-Terrorism Council and Department of Trade and Industry), among others.

STAGE 2: RISK ANALYSIS

The procedure entails conducting a meticulous and knowledgeable assessment of the characteristics, origins, probability, and implications of the identified risks. This entails considering different techniques to determine the level and severity of each risk, such as evaluating their extent and relative importance or employing a more formal method such as a likelihood and impact matrix. This approach allows ICREs to effectively allocate relative value or risk level to each ML/TF/PF or sanctions risk.

a. Likelihood Assessment

This determines the probability or chance of the risk to occur based on its nature and sources, as well as the overall vulnerability of the ICRE with respect to the risk. The ICRE may use a likelihood matrix to indicate the assessed level of occurrence. Sample likelihood rating and assessment are shown below:

Figure 8. Sample Likelihood Rating

Rating	Description
High	There is a **high** probability that the identified ML/TF/PF/sanctions risks will occur (very likely).
Moderate	There is a **moderate** probability that the identified ML/TF/PF/sanctions risks will occur (possible).
Low	There is **low** probability that the identified ML/TF/PF/sanctions risk will occur (unlikely).

Figure 9. Sample Likelihood Assessment of a Threat

An ICRE assessed a "high" likelihood that it will be used for OSEC-related crimes due to: (i) a high volume of remittance transactions from countries and regions that are known as sources and destinations of the proceeds of crime, (ii) high exposure to the sector/types of clients that are possibly engaged in OSEC, and (iii) insufficient monitoring process to identify and track OSEC related activity.

b. Impact Assessment

This provides an analysis of the consequence or impact of the risk to the ICRE. This may be quite challenging, but it will allow the ICRE to focus its resources efficiently. ICREs may consider the potential consequences of ML/TF/PF activities on the following aspects, as applicable:

i. Financial impact (e.g., operational losses and penalties incurred)
ii. Reputational impact (e.g., adverse media report that could damage the name, brand, or industry)
iii. Employee impact (e.g., high employee dissatisfaction and loss of key staff)
iv. Customer impact (e.g., loss of trust and loss of customer funds/income)

Depending on the complexity and risk profile of the ICRE, it may adopt a risk rating scale to reflect the severity of the impact of the key risk or threat if it occurs. Example of impact assessment is shown in Figure 10.

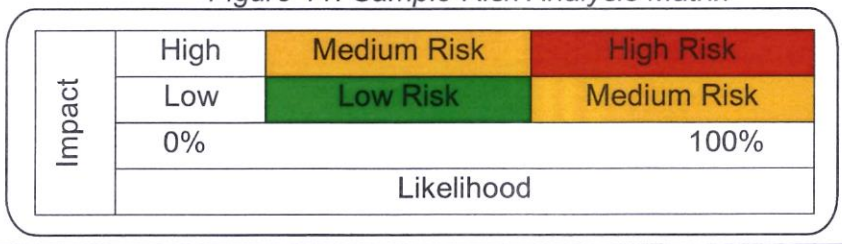
Figure 10. Sample Impact Rating Assessment

Level	Impact on		
	Financial	**Reputational**	**Customer**
Major	Significant losses/ reduction in stock price/penalties	Prolonged adverse media attention	Significant loss of trust/financial loss
Moderate	Manageable losses/ reduction in stock price/penalties	Modest/controlled adverse media attention	Modest loss of trust/financial loss
Minor	Minimal losses/ penalties	No media coverage	Minimal losses to customers/no loss of trust

c. Level of Risk

An estimate of the level of each identified risk can be determined based on the assessment of its likelihood of occurrence and the impact. A simple risk analysis matrix is shown in Figure 11.

Figure 11. Sample Risk Analysis Matrix[4]



High Risk - There is a high chance of ML/TF/PF occurring in this area, and the impact on the business is high in terms of financial, reputational, or customer impact.

Medium Risk - There is a high chance of ML/TF/PF occurring in this area, but the impact on the business is low, or there is a low chance of ML/TF/PF occurring in this area, but the impact on the business, if it will occur, is high.

Low Risk - There is a low chance of ML/TF/PF occurring with little or negligible impact on the business.

d. Quality of Risk Management (QRM) Assessment

This part assesses the extent and adequacy of existing ML/TF/PF risk management framework or controls relative to the identified risk level. This may involve assessing the following, among others:

i. Quality of BOD and senior management oversight;
ii. Adequacy of the MTPP;
iii. Effectiveness of internal controls and its implementation. This includes assessment of onboarding customer due diligence (CDD), ongoing monitoring of accounts and transactions, implementation of TFS, compliance with freeze orders, covered and suspicious transaction reporting, record keeping, and AML/CTPF training program; and
iv. Effectiveness of self-assessment functions (audit and compliance units).

[4] Source: FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment, February 2013

To mitigate the identified risks or threats, the ICRE should implement relevant risk-based controls or measures. Gathering the necessary documents and information to support the analysis is crucial. These documents can include the ICRE's policies and procedures, processes, systems, monitoring tools, resource allocation, training information, and sanctions imposed.

The overall effectiveness of the QRM should be linked to the assessment conducted by the Audit and Compliance units, as well as the results of the IC examinations. The assessment of the QRM should focus on identifying strengths and weaknesses or gaps in the risk management framework that drive the overall rating. This information will be valuable in developing an action plan to address any identified weaknesses.

Figure 12. Identifying/Assessing Control Risk Factors

Some ICREs use the following as part of control assessment:

1. A survey questionnaire is issued to different assessed units. Each control factor, such as culture and governance, staffing and resources, policies and procedures, CDD, enhanced due diligence (EDD), name screening, monitoring, reporting, training and awareness, technology systems, quality assurance, and testing and audit, are evaluated on a per-unit basis.

2. Focus group discussion is conducted on documented controls for each of the key risk factors, e.g., product risk assessment discussion on limits, approvals, transaction monitoring, and conduct of EDD.

Figure 13: Sample QRM Assessment

Rating	Description
Strong	Highly effective and needs minor improvements
Acceptable	Substantial level of effectiveness and needs moderate improvements
Inadequate	Not effective and needs major improvements
Weak	No control or needs fundamental improvements

ICREs need to evaluate their existing controls to mitigate TFS risks arising from potential breach, non-implementation, or evasion. The ICRE should assess the following:

(i) the adequacy and appropriateness of sanctions policies, systems, and controls;
(ii) the extent, availability, and timely updating of screening databases and tools;
(iii) their capability to screen prospective customers, including those securing insurance contracts, pre-need and HMO products through online applications, existing customers, all relevant parties in a payment chain, walk-in clients, and other counterparties;
(iv) the effectiveness of freezing and prohibition rules implementation; and
(v) their ability to implement TFS promptly.

e. Residual Risk

Residual risk is the risk that remains after systems and controls are applied to the identified and assessed inherent risk level. The residual risk rating is crucial as it reflects whether identified ML/TF/PF risks are adequately managed or are within the ICRE's risk appetite. It will also dictate if action plans or further preventive measures or controls are warranted.

Residual Sanctions Risk

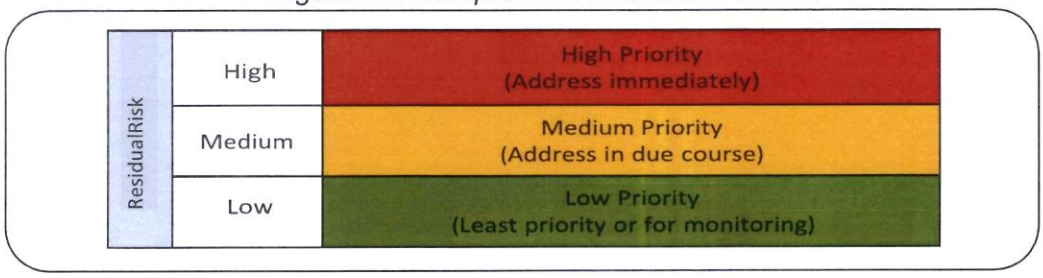
When assessing residual risk for sanctions, it is essential to use the same approach as ML/TF/PF. However, some ICREs may opt to conduct separate assessments for sanctions risk due to the differing scope and purpose. This targeted approach allows for a more focused analysis of sanctions and terrorist financing risks and the adequacy of controls to meet regulatory requirements. When presenting findings on residual sanctions risk, it is important to identify the drivers of inherent risk, its potential impact and likelihood, and the effectiveness of existing control measures. For example, the assessment may reveal instances where the institution cannot identify sanctioned individuals and entities despite using screening tools. It may also highlight certain products, services, channels, or customer types that are not adequately covered by current screening measures, leading to a high impact due to potential severe penalties.

STAGE 3: RISK EVALUATION

In this phase, it is important to identify priorities and create effective strategies that align with the level of identified residual risks in the prior risk analysis stage. The residual risk should be in line with the established risk appetite of the ICRE. Thus, depending on the risk appetite, the ICRE must employ methods to address identified risks, including

acceptance, prevention (such as prohibiting certain products, services, or activities), or mitigation (or reduction). A simple risk evaluation matrix is shown in Figure 14.

Figure 14. Sample Risk Evaluation Matrix



It is important to prioritize high-risk situations by allocating the highest level of resources and urgent action and monitoring required to mitigate risks effectively. Medium-risk should also receive a significant level of resources and attention, while those at low risk may require fewer resources and less immediate action. This approach ensures that resources are allocated based on the level of risk, allowing for an effective mitigation of potential risks.

Less complex ICREs might choose to use a straightforward approach that involves identifying threats and vulnerabilities, conducting risk analysis, and then developing action plans and strategies. This could involve adjusting or improving AML/CTPF policies, procedures, systems, and controls. The action plan should be specific, measurable, achievable, relevant, and time-bound, taking into account the level of residual risks identified.

In line with the risk-based approach, it is expected that where there are higher risks, ICREs should take enhanced measures to manage and mitigate those risks. Correspondingly, where the risks are lower, simplified measures may be permitted.

Simplified measures should not be permitted whenever there is a suspicion of ML/TF/PF[5]. Examples of controls include setting transaction limits/thresholds for high-risk products/services, requiring management approval for high-risk transactions or clients, or restricting and/or prohibiting clients that are beyond the ICRE's risk appetite.

4. REPORTING

The IRA report, containing the assessment results and recommendations, must be submitted to the BOD for approval. The findings and any action plans or amendments to the ICRE's AML/CTPF policies and procedures to mitigate

[5] FATF Recommendation 1 Interpretative Note

identified risk should be timely communicated to concerned personnel to foster shared understanding and effective implementation.

Figure 15. Sample Outline of an IRA Report

i. Overall risk assessment for each threat/risk identified
ii. Factors that drive the risk assessment
iii. Overview of mitigating measures
iv. Action plans to mitigate the risks
v. Methodologies used
vi. List of units which participated in the risk assessment

5. MONITORING AND RE-ASSESSMENT

The ICRE should establish effective systems and processes to ensure that action plans are implemented and AML/CTPF policies, controls, and procedures are revised in line with the identified risks. It is important to clearly define responsibilities for implementing and monitoring the action plan to ensure accountability. These efforts should be included as part of the management's regular report to the Board of Directors.

The IRA is expected to be up-to-date. IRA shall be conducted, at least once every two years, or as often as the BOD or senior management may direct, depending on relevant factors/developments. Examples of triggers include:

a. Newly-identified financial crime threats and emerging trends on the products and services being offered;
b. Changes in business operation (i.e., mergers, consolidation, etc.); and
c. Significant increase in volume and value of transactions and STRs.

A critical part of updating the IRA involves thoroughly reviewing the suitability of the IRA methodology, ensuring that the data, information, and reports used in the assessment are adequate, and calibrating the assumptions used. This ensures that the IRA exercise will yield meaningful and reasonable results for the ICREs.

6. NEW PRODUCTS/SERVICES

ICREs are also required to conduct risk assessment in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

In the conduct of inherent risk of the new products/services, ICREs should consider the functionalities/features of the products and services, and target market/customers, among others. Some factors that may elevate risks include the presence of features that

allow customer anonymity, disguised and/or concealed beneficial owners and sources of funds and wealth of customers, large cash transactions, or movement of funds across borders.

To arrive at the residual risk, the ICRE should consider controls relevant/related to the inherent risk of the new products and services. If the residual risk is high, the ICRE should institute additional controls, such as a) providing transaction limits, b) requiring approval of higher authority, c) conducting further due diligence on transactions that exceed thresholds, and/or d) providing only the product to certain/specific target market (e.g., low -risk profile market), among others, prior to deployment of the products/services.

ANNEX A

FACTORS, INFORMATION/DATA AND ASSESSMENT CONSIDERATIONS

The data and information indicated herein are examples only and are not exhaustive. Other factors, data, and information should be gathered to support the risk assessment process.

Factors	Relevant Data	Sample High Risk Indicators and Considerations
Products and Services	a. Transaction Volume and Value of products sold for CY __, product type/services, description of risk, % Ratio Annualized Premium Equivalent b. Covered and suspicious transactions reports (CTRs/STRs) c. Freeze Order, Asset Preservation Order, and Civil Forfeiture d. National and Sectoral Risk Assessments (NRA/SRA) and other related studies/ typologies provided by relevant government agencies	a. Possible high risk indicators for products and services include: i allow client anonymity ii accept disguised and/or concealed beneficial owner, source of fund and wealth of customer iii allow customer to conduct business with higher risk business segments or to use the product/service on behalf of third parties iv involve receipt and payment in high volume of cash v allow movement of funds swiftly and across borders vi identified in the NRA/SRA as presenting high risk b. Consider the value and volume of the transactions related to the products/services. Determine which products and services were commonly involved in STRs, freeze orders, asset preservation orders, or civil forfeiture. c. New or innovative products or services that are not provided directly by the entity but are provided through channels. d. Services identified by internationally recognized and credible sources as being high-risk. e. Life insurance policies, pre-need and HMO products with back-to-back loans (if applicable), trade finance, and other high-quality, complex products may produce a higher risk because of their complexity or lack of transparency.
Customers	a. Customer Transaction volume and value for CY ___type of customers, description of risk, % Ratio Annualized Premium Equivalent b. Nature, source of funds or wealth of customers c. Number of customers per risk category, customers involved in reports/negative information or the types of customers that are	a. Number of high-risk customers and/or clients for each product/service assessed. For example, if most clients are low to normal risk, and that the value and volume of transactions of high-risk clients are minimal, this may support a low-to-normal risk assessment of customers. b. Nature/category and number of customers involved in STRs, freeze orders, and asset preservation orders. This may heighten risk posed by customers. c. Customers who conduct their business relationships or transactions or who have these conducted under unusual circumstances, such as an unexplained geographic distance between the ICRE and the location of the customer,

	normally engaged in illegal activities d. Number of clients from high-risk regions or jurisdiction e. NRA, SRA and other related studies or typologies	frequent and unexplained transfers of accounts in various geographic locations. d. Please see Indicators of Suspicious Transactions, "Annex A" of CL No. 2018-48.
Geographic Location	a. Value and volume of transactions with certain countries that are known high risk to ML/TF/PF based on NRA, SRA or other typologies b. TF risk assessment, external threat assessments, and other relevant risk assessments	a. Consider regional and country risks. Identify high-risk countries based on relevant sources such as NRA, SRA, and other studies conducted by relevant government agencies. FATF list of high-risk and non-cooperative jurisdictions. FATF mutual evaluation reports. United Nations Office on Drugs and Crimes reports, and UNSCR resolutions. b. Based on the list of high-risk regions or jurisdictions, determine the number of branches and offices therein and data on clients and their transactions from said jurisdictions. Significant exposure to these regions or countries will elevate the risk related to geographic location. Nonetheless, not all clients from high-risk regions or jurisdictions pose a high risk. ICRE should understand how this will affect the clients' transactions. c. Countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activity including source or transit countries for illegal drugs, human trafficking and smuggling, and illegal gambling. d. Geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities. e. Geographic areas identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.
Delivery Channels and Transactions Risk	a. Available delivery channels b. Payment channels c. Types and number of customers using the delivery channels d. Platforms posing higher risk based on NRA, SRA, and other relevant risk assessments, studies, or reports	a. Possible Indicators that may heighten risk for channels include: i. New technology/new payment methods ii. Non-face-to-face contact during onboarding (ICRE can assess whether the customer is physically present for identification purposes. If they are not, ICRE may use reliable forms of non-face-to-face customer due diligence and the extent the ICRE has taken steps to prevent impersonation or identity fraud.) iii. Products and services are provided via the Internet.

		iv. ICRE has indirect relationships with customers (via intermediaries, pooled accounts, etc.) v. Products/services are provided through agents, intermediaries, or third parties. vi. Facilitate cross-border transactions vii. Determine the number of customers onboarded and/or who are using the channels with heightened ML/TF/PF risks.
Sanction Risk	a. Indirect exposure to embargoed jurisdictions or entities included on various sanctioned lists b. Availability of sanctions screening system c. Number of customers under sanctioned list d. Number of potential match or target match generated e. Number of STR, account frozen f. Number of asset preservation orders received from AMLC or Law Enforcement Agencies (LEAs)	a. The Jurisdiction where the ICRE is located, and its proximity geographically, culturally, and historically to sanctioned countries. b. Kind or types of customers the ICRE has international or domestic, where those customers are located, and what business they undertake. c. The volume of transactions and distribution channels. d. Kind of products and services offered and whether those products represent a heightened sanctions risk (ex. Cross-border transactions, foreign correspondent accounts, trade-related products, or payable-through accounts).

ANNEX B

SAMPLE PARAMETERS FOR RISK CLASSIFICATION

Factors	Low	Moderate	High
Products and Services	• Traditional Insurance products or services • Whole Life, Endowment, Term Insurance • Few or no significant transactions • Catered only to low risk types of customers • No cross-border element • Does not allow client anonymity	• Minimal to modest products or services offered pose higher ML/TF/PF risks as identified in NRA, SRA, and other relevant assessments • Moderate level of transaction volume and value	• Full or wide range of products or services including those posing higher ML/TF/PF risks • VUL Products • Marine Products, Trade Finance and other high risk products • Large value and volume of transactions • Products cater to all types of clients and/or allow client anonymity • Significant number of transactions are filed as STR or subject to freeze orders • Significant cross-border transactions
Client Base Profile /Customers	• Low number of customers or high risk customers • Low volume/value of activity, aggregate balance • Simple transactions	• Modest number of customers or high risk customers	• Significant number of customers/high risk customers
Delivery Channels /Payment Channels and Transactions	• Client onboarding and/or transaction is performed via face-to-face verification	• Some products and services are offered via electronic channels • Modest number of accounts are opened via third party, agents, outsourced parties, or via electronic channels	• Most products/services are offered via electronic channels • Client on-boarding is mostly conducted by outsourced parties or third parties or agents and/or via electronic channels without face-to-face contact/verification Payments through Pay Maya, Gcash, or other payment channels
Geographic Location	• Minimal number of branches and/or clients in high risk regions/ countries • Minimal value and volume of transactions in high risk areas	• Modest number of branches, clients and/or level of transactions in high risk regions/countries	• Significant number of branches and/or clients in high risk regions, countries or Domestic branches under high risk areas • Large value and volume of transactions in high risk areas