BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2022-030

To : **All BSP Supervised Financial Institutions**

Subject : **Guidance Paper on the Conduct of Institutional Risk Assessment (IRA)**

Section 911/911-Q of the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions require BSP-supervised financial institutions (BSFIs) to identify, understand, and assess the money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks arising from their respective business operations.

This Guidance Paper provides practicable insights in the conduct of IRA to achieve optimal results that will inform risk-driven approach in the design and implementation of preventive measures to detect and mitigate ML/TF/PF and sanctions risks.

The Guidance Paper outlines, among others, the governing rules and international standards, regulatory expectations, and the IRA process. This was informed by, among others, existing laws, rules and regulations governing IRA, relevant documents issued by standard setting bodies and regulators as well as observed best practices in the conduct of IRA. It must be emphasized that in conducting the IRA, there is no one-size-fits-all approach and the methodology should be tailored fit to the nature and complexity of the BSFI's activities and operations.

BSFIs are enjoined to consider this guidance paper in the conduct of the IRA and take commensurate preventive measures in line with their risk posture.

Digitally signed by
DG Chuchi G. Fonacier
30 June 2022

CHUCHI G. FONACIER
Deputy Governor

30 June 2022

Guidance Paper on the Conduct of

INSTITUTIONAL RISK ASSESSMENT

June 2022

GUIDANCE PAPER ON THE CONDUCT OF INSTITUTIONAL RISK ASSESSMENT

TABLE OF CONTENTS

GUIDANCE PAPER ON THE CONDUCT OF INSTITUTIONAL RISK ASSESSMENT

INTRODUCTION

Institutional Risk Assessment (IRA) is the cornerstone of risk-based approach to money laundering (ML), terrorist financing (TF), proliferation financing (PF), and sanctions risks prevention and mitigation. The IRA is a process using appropriate methodology to identify, analyze and understand the ML/TF/PF risks, including the risk of non-implementation, potential breach, or evasion of targeted financial sanctions (TFS) requirements, arising from the BSP-supervised financial institution's (BSFI's) business activities and relationships. Its results should guide the development and/or enhancements of anti-money laundering and countering terrorist and proliferation financing (AML/CTPF) policies, systems, controls, and procedures, and inform efficient and risk-focused allocation of AML/CTPF resources. This ensures that AML/CTPF policies, systems, controls, and procedures are suited to the BSFI's operations and risk posture.

This document sets out the regulatory expectations and provides practical guidance and insights to assist BSFIs in the conduct of their IRA, considering existing regulations, relevant international standards, and industry best practices. It presents a general approach that is flexible and can be tailored fit to the nature and complexity of BSFIs' activities and operations, including those with simple business models.

A. 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* – Covered persons shall take appropriate steps to identify, assess, and understand their ML/TF risks.

2. *Section 911/911-Q of the Manual of Regulations for Banks/Non-Bank Financial Institutions* – Consistent with risk-based approach, covered persons are required to identify, understand, and assess their ML/TF risks, arising from customers, countries or geographic areas of operations/customers, products, services, transactions, or delivery channels.

3. *Financial Action Task Force (FATF) Recommendation 1* provides that countries should, among others, require financial institutions and designated non-financial businesses and professions (DNFBPs)[1] to identify, assess, and take effective action to mitigate their ML/TF/PF risks.

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 TF.

5. *FATF Recommendation 7* necessitates the implementation of TFS to comply with the UNSC resolutions relating to the prevention, suppression and disruption of 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.*

[1] Based on the FATF Glossary, DNFBPs mean: (a) Casinos; (b) Real estate agents; (c) Dealers in precious metals; (d) Dealers in precious stones; (e) Lawyers, notaries, other independent legal professionals, and accountants; and (f) Trust and Company Service Providers

B. OBJECTIVES OF THE IRA

The IRA facilitates the identification of the sources of ML/TF/PF and sanctions threats/risks, the vulnerabilities of the BSFI's business/operations, the assessment of the existing controls to prevent or mitigate such risks, the determination of the residual risk and evaluation of corresponding action plans. BSFIs should craft bespoke policies, controls, and procedures to effectively manage and mitigate the identified risks. This results in a risk-driven ML/TF/PF prevention and mitigation strategy. Specifically, the results of the IRA are valuable as they, among others:

1. Present to the Board of Directors (BOD) and Senior Management information on the BSFI'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[2] of the BSFI;

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 which present higher risks such that where higher risks are identified, enhanced measures should be taken to manage and mitigate the risks; and

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

C. REGULATORY EXPECTATIONS ON IRA

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

1. The IRA shall (a) use a methodology that is suited to the BSFI'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.

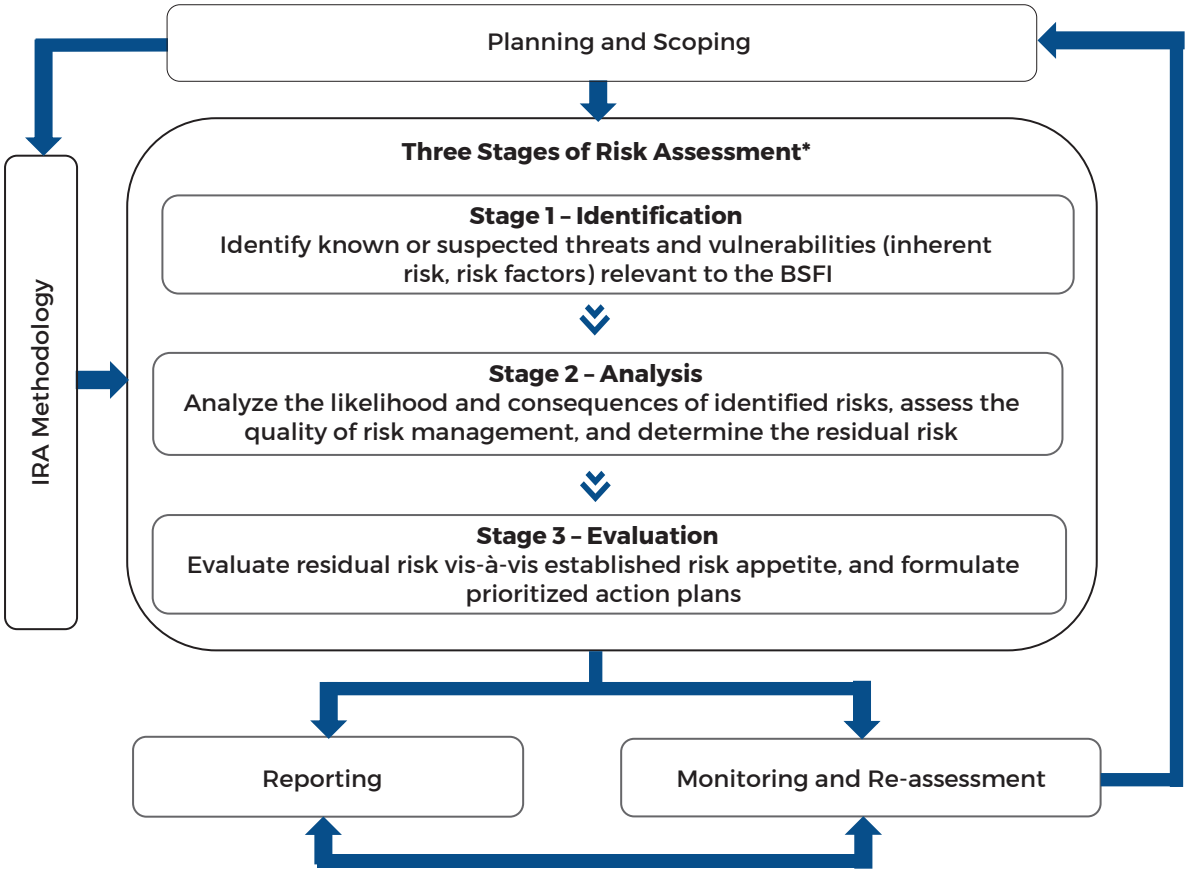
2. BSFIs are required to identify and assess the ML/TF/PF and sanctions risks that may arise in relation to the development and/or introduction of new products/services, business practices, delivery channels and technologies. Such risk assessment should be an integral part of the product or service development process and be performed prior to the launch of the new products, business practices or the use of new or developing technologies.

3. Based on the results of the IRA and/or new product or business practices risk assessment, BSFIs shall take appropriate measures to manage and mitigate the identified ML/TF/PF and sanctions risks, including enhanced measures on those categorized as high risks areas, which should be clearly articulated in the MTPP.

4. The risk assessment shall be made available to the BSP during examination or in other instances deemed necessary as part of risk-based supervision.

[2] Risk appetite is the aggregate level and types of risk a BSFI is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan (Basel Committee on Banking Supervision 2015 Corporate governance guidelines)

D. IRA PROCESS



*Note: *The three stages are generally based on the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (2013).*

Key Terms[3]

Threat – a person or group of people, object, or activity with the potential to cause harm to, for example, the state, society, or economy, etc. In ML/TF/PF context, this includes criminals, terrorist groups, and their facilitators.

Vulnerabilities – comprise those things that can be exploited by the threat or that may support or facilitate its activities. In ML/TF/PF risk assessment context, these may include features of a financial products/services that make them attractive for ML/TF/PF.

Consequence – refers to the impact or harm that the ML/TF/PF may cause and includes the effect of underlying criminal and terrorist activity on the financial system, the institution, or its customers.

Risk Factors – specific threats or vulnerabilities that are the causes, sources, or drivers of ML/TF/PF risks.

[3] Based on FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment, February 2013

1. PLANNING AND SCOPING

A systematic process is important to a meaningful ML/TF/PF and sanctions risk assessment. BSFIs 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. It is essential that there should 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 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. BSFIs 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.

Box 1. IRA Team

> In one BSFI, the Compliance Office leads the conduct of the IRA, supported by the BOD, senior officers, and heads of relevant business units such as Branch Banking and Corporate Banking Groups, 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. It is imperative that relevant quantitative and qualitative data or information are 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 BSP 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]). It is advisable that BSFIs develop 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.

Box 2. Survey Questionnaire

> A BSFI 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

Another essential aspect of the IRA process is the use of a suitable methodology. There is no "one-size-fits-all" approach in assessing ML/TF/PF and sanctions risks. The risk assessment methodology that the BSFI adopts should be proportionate to the nature and complexity of its activities and operations. For example, complex BSFIs are expected to have a more detailed or sophisticated assessment process while smaller or less complex BSFIs may use simple methodology. The primary consideration is that the adopted methodology reasonably captures and analyzes the BSFI's real risk posture and achieves the defined objectives of the assessment.

Box 3. Risk Assessment Methodology

A BSFI uses a risk assessment methodology which measures ML/TF/PF risks based on threat, vulnerability, and consequences. The BSFI 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 BSFI.

3. THREE STAGES OF THE RISK ASSESSMENT PROCESS

STAGE 1: RISK IDENTIFICATION

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

a. Identifying ML/TF/PF Threat

This involves understanding the threat environment and listing known threats, such as relevant predicate offenses and their proceeds. It includes gathering of information related to known or suspected threats and sectors, products or services that have been or may be exploited. In identifying threats, BSFIs may refer to various sources, such as the a) results of the NRA/SRA, which usually provide information on, among others, the ML/TF/PF threat environment and the financial services used in the proceeds of illegal activities; b) analysis of suspicious transaction reports (STRs), fraud cases filed, as well as freeze orders, bank inquiries, and asset preservation orders received; and c) news article, reliable reports or published studies on ML/TF/PF and sanctions typologies.

Box 4. Sample Threat Guide Questions

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

Box 5. Sample Risk Scenario of a Bank

A Bank 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 banking 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[4]), and taking appropriate mitigating measures commensurate with the level of identified risks[5].

TFS requires asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities[6]. It must be highlighted that TFS implementation is rule-based as full application of the TFS is required. Nonetheless, TFS risk assessment informs identification of risk-based measures that the BSFIs shall take to reinforce and complement the full implementation of the 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

Inherent risk refers to the level of intrinsic ML/TF/PF and sanctions risks, before the introduction of controls or preventive measures, arising from the BSFI's business and relationships. Key drivers of inherent risk in the business include the nature, scale, features and complexity of the products or services offered, delivery channels, and geographical location of the BSFI's operations, as well as new developments and technologies related to the operations, among others. Relationship-based risk assessment focuses on the customers and the BSFI's business relationships with them, including the products, services, and delivery channels they avail or utilize, geographic location of the customer and their transactions, new developments, or technologies available to them and historical patterns of customers' transactions.

BSFIs should identify inherent risk in accordance with their adopted methodology. This entails gathering of data and/or information to assess each key element such as the nature, depth, scale, features, diversity and geographic footprint of the business, target market, customer profiles, and value and volume of transactions. Annex A provides an illustrative example of data or information to support inherent risk identification. It is also expedient to utilize a scoring system for each of the inherent risk factors, with appropriate parameters, threshold, and assumption to support the rating system. This should be tailored to the size and type of the business operations of the BSFI. Annex B provides sample parameters for risk classifications for illustrative purposes.

Based on the scoring used, the BSFI will be able to identify the overall level of ML/TF/PF inherent risk and provide a statement on what factor/s or element/s significantly drive the inherent risk. For example, the vulnerability of a BSFI to ML threat related to OSEC can be assessed by analyzing the inherent risk of its remittance product, types of clients, and geographic risk (e.g., the value and

[4] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf
[5] https://www.fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing-2020.html
[6] 2021 AMLC Sanctions Guidelines, Chapter 1

volume of transactions to and from countries known for OSEC, and the extent of clients that are possibly related to OSEC-related crime). Illustrative examples of inherent risk scoring and assessment matrix are shown in Boxes 6 and 7, respectively.

Box 6: Example of Inherent Risk Scoring

A BSFI adopts a risk scoring that considers inherent risk factors with equivalent risk point 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

Box 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 inherent risk
Low	Marginal level of inherent risk

TFS Inherent Risk

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

i. *Relevant sanctions lists*. Sanctions risk exposures to domestically-designated personalities and those in the UNSC resolutions on TF and PF. TFS requirements are rule-based, which means full application of TFS. Meanwhile, BSFIs 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 high prevalence of terrorism, TF and PF related activities. This can be sourced from relevant reports such as NRA/SRA, regional risk assessment 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

This involves a thorough and informed assessment of the nature, sources, likelihood, and consequences of the identified risks. This may involve determination of the level and seriousness of each risk using different techniques, for example, in terms of their degree and relative importance, or a more formal technique using a likelihood and impact matrix. It will facilitate the assignment of relative value or risk level for each of the identified ML/TF/PF or sanctions risks.

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 BSFI with respect to the

risk. The BSFI may use a likelihood matrix to indicate the assessed level of occurrence. Sample likelihood rating and assessment are shown below:

Box 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 **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).*

Box 9. Sample Likelihood Assessment of a Threat

A BSFI assessed a "high" likelihood that it will be used for OSEC-related crimes due to: (i) 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 BSFI. This may be quite challenging, but it will allow the BSFI to focus its resources efficiently. BSFIs 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 BSFI, it may adopt a risk rating scale to reflect the severity of impact of the key risk or threat if it occurs. Example of impact assessment is shown in Box 10.

Box 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 Box 11.

Box 11. Sample Risk Analysis Matrix[7]

Impact			
	High	Medium Risk	High Risk
	Low	Low Risk	Medium Risk
	0%		100%
	Likelihood		

High Risk - There is a high chance of ML/TF/PF occurring in this area, and the impact to 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 to the business is low; or there is low chance of ML/TF/PF occurring in this area, but the impact to 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 to 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).

The BSFI should consider the relevant and risk-based controls or measures to mitigate the identified risks or threats. Necessary documents and information should be gathered to support the analysis. Examples of such documents include the BSFI's policies and procedures, processes, systems, monitoring tools, resource allocation, training information, and sanctions imposed. The overall effectiveness of the QRM should be correlated with the assessment conducted by the Audit and Compliance units, as well as results of the BSP examinations. Assessment of the QRM should cover the identification of strengths and weaknesses or gaps in the risk management framework that drive the overall rating. This will be useful in the development of an action plan to resolve identified weaknesses.

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

Box 12. Identifying/Assessing Control Risk Factors

Some BSFIs 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, is 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, and transaction monitoring, and conduct of EDD.

Box 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

For TFS risk, BSFIs need to evaluate the existing controls in place to mitigate the risks arising from potential breach, non-implementation or evasion of TFS. The BSFI should consider, among others, the: (i) adequacy and appropriateness of sanctions policies, systems and controls; (ii) extent, availability and timely updating of screening database and tools; (iii) capability to screen prospective and existing customers, all relevant parties to a payment chain, walk-in clients, and other types of counterparties; (iv) effectiveness of implementation of freezing and prohibition rules; and (v) ability to implement TFS without delay.

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 is within the BSFI's risk appetite. It will also dictate if action plans or further preventive measures or controls are warranted.

Residual Sanctions Risk

The procedure in determining the residual risk for sanctions risk is the same as that related to ML/TF/PF. Some banks conduct separate sanctions risk assessment due to its different scope and purpose. This allows the BSFI to focus on the identification of sanctions/TFS risk and exposures, and the suitability of controls to comply with TFS requirements. In providing conclusion on residual sanctions risk, the BSFI should be able to indicate the drivers of the inherent risk, its impact and likelihood, as well as the effectiveness of the control measures that are in place to mitigate sanctions risks. The residual risk may indicate, for example, that the BSFI cannot identify sanctioned individuals and entities even after adopting screening tools, or there are certain products and services, channels, and or types of customers that are not subjected to the existing screening tools of the BSFI, and that the impact is high due to corresponding high penalties, among others.

STAGE 3: RISK EVALUATION

This stage involves determining priorities and developing applicable strategies commensurate with the level of assessed residual risks in the risk analysis stage. Residual risk should be within the BSFI's established risk appetite. Thus, depending on the level of risk appetite, the BSFI must employ methods to address identified risks such as acceptance, prevention (e.g., prohibiting certain products, services, or activities), or mitigation (or reduction). A simple risk evaluation matrix is shown in Box 14.

Box 14. Sample Risk Evaluation Matrix

Residual Risk		
	High	High Priority (Address immediately)
	Medium	Medium Priority (Address in due course)
	Low	Low Priority (Least priority or for monitoring)

Those falling under high risk will require the highest priority for allocating resources in terms of action needed to respond to the risk, urgency of response, efforts and monitoring required to mitigate the risks. Meanwhile, for those falling under medium risk, the BSFI is also expected to allot a commensurate or moderate level of resources in terms of action, urgency of response, efforts, and monitoring. Lastly, those that would fall under low risk could be the least priority in terms of resources and action. In essence, this will result in a risk-driven approach in mitigating risks.

Simple or less complex BSFIs may adopt simpler methodology that will basically cover the identification of threats and vulnerabilities, and risk analysis to arrive at the development of appropriate action plans and strategies. This may include calibrating or enhancing the AML/CTPF policies, procedures, systems, and controls. The action plan should be specific, measurable, attainable, relevant, and time bound considering the level of identified residual risks.

In line with risk-based approach, it is expected that where there are higher risks, BSFIs 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[8]. 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 BSFI's risk appetite.

4. REPORTING

The IRA report, which contains the results of the assessment and corresponding recommendations, among others, shall be reported to and approved by the BOD. Its results as well as the action plans or amendments to the BSFI's AML/CTPF policies and procedures to reduce identified risk should be timely disseminated/cascaded to concerned personnel to foster shared understanding and effective implementation.

[8] FATF Recommendation 1 Interpretative Note

Box 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 BSFI is expected to institute systems and processes to ensure implementation of the action plans and/or revise AML/CTPF policies, controls, and procedures commensurate with the identified risks. Responsibilities for the implementation and monitoring of the action plan should be identified to assign accountabilities. This should form part of the Management's periodic report to the BOD.

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.

Critical part of updating the IRA is the review of the suitability of the IRA methodology and adequacy of data, information and reports used in the assessment, as well as calibration of assumptions used. This ensures that the IRA exercise will provide reasonable and meaningful results to the BSFI.

6. NEW PRODUCTS/SERVICES

BSFIs 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, BSFIs should consider the functionalities/features of the products and services, and target market/customers, among others. Some factors that may elevate risks include presence of features that allow customer anonymity, disguised and/or concealed beneficial owner and source of fund and wealth of customer, large cash transactions, or movement of funds across borders.

To arrive at the residual risk, the BSFI should consider controls relevant/related to the inherent risk of the new products and services. If the residual risk is high, the BSFI 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. Value and volume of deposits, loans, remittances, foreign exchange transactions, and other products and services, as applicable b. Covered and suspicious transactions reports (CTRs/STRs) c. Freeze Order, Bank Inquiry, 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. c. Determine which products and services were commonly involved in STRs, freeze orders, bank inquiry[1] or civil forfeiture.
Customers	a. Nature, source of funds or wealth of customers b. Number of customers per risk category, customers involved in reports/negative information or the types of customers that are normally engaged in illegal activities c. Number of clients from high-risk regions or jurisdiction d. NRA, SRA and other related studies or typologies	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 customer. b. Nature/category and number of customers involved in STRs, freeze orders, bank inquiry. This may heighten risk posed by customers.
Geographic Location	a. Value and volume of transactions with certain countries that	a. Consider regional and country risk. Identify high risk countries based on relevant sources such as NRA, SRA and other studies

[1] BSFIs should protect the confidentiality and avoid tipping off of information from bank inquiry being conducted by AMLC when relevant information is used for the IRA exercise.

Factors	Relevant Data	Sample High Risk Indicators and Considerations
	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	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 a high risk region or jurisdiction pose high risk. BSFI should understand how this will affect the clients' transactions.
Delivery Channels	a. Available delivery channels b. Types and number of customers using the delivery channels c. 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 iii. Facilitate cross-border transactions iv. Use of intermediaries, agents, or third parties b. Determine the number of customers onboarded and/or who are using the channels with heightened ML/TF/PF risk.

ANNEX B

SAMPLE PARAMETERS FOR RISK CLASSIFICATION

Factors	Low	Moderate	High
Products and Services	• Traditional banking products or services • 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 • 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	• 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	• 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
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 the high risk regions or countries • Large value and volume of transactions in high risk areas