هيئة السوق المالية
Capital Market Authority

Business Risk Assessment Guideline

Capital Market Authority

This guide is intended for guidance purposes only and does not replace, nor should it be construed as a substitute for, the provisions contained in the regulations, rules, and instructions in force at the Capital Market Authority. In the event of any conflict between the content of this guide and the provisions of those regulation and rules, the latter shall prevail as the authoritative reference.

Glossary of Terms	
AML/CFT/CPF	Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing
Risk-based Approach (RBA)	Identifying, assessing and understanding ML/TF/PF risks to which an FI is exposed and take AML/CFT/CPF measures commensurate to those risks to mitigated them effectively and efficiently.
Financial Action Task Force (FATF)	an intergovernmental organization that sets international standards and promotes policies to combat money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction
Business Risk Assessment (BRA)	An exercise which identifies the risk of ML/TF/PF posed to the FI as a whole based on its activities
Customer risk assessment (CRA)	An exercise which identifies the risks that each individual customer (individual or legal person) poses to the business.
Inherent Risk	The risk of ML/TF/PF occurring without consideration of any controls or mitigants
Preventative/Risk Mitigation Measures	The controls which are in place to mitigate the existence of risks or to prevent risks from materializing.
Residual Risk	The risk that remains after all control measures have been implemented effectively
Risk Appetite	The level of risk the FI is prepared to accept in the course of its business operations.
Trigger Event	A specific event or action that prompts an ad hoc review of the BRA
Structural risk	Risks arising from the entity's ownership structure, governance framework, and operational complexity
Customer Risk	The level of risk posed by the entity's customer base
Product, Services, Transaction Risk	Risks associated with the nature of the products and services offered, as well as the complexity, volume, and frequency of transactions
Delivery Channel Risk	The risk posed by the methods used to deliver products and services
Geographic Risk	Risks linked to the jurisdictions in which the FI operates, conducts transactions, or has business relationships
Emerging risk	New and developing risks associated with individual sectors

Non-Profit Organisation (NPO)	A Legal entity that engages in collecting, receiving, or paying money for charitable, religious, cultural, educational, social, or solidarity purposes or that conduct other charitable activities.
Preventative Controls	Those controls that limit the ability to use the product or channel in a way that would increase the ML/TF/PF risks
Detective Controls	Controls that monitor activity through the product or channel.

Purpose and Scope

1. The purpose of this Guideline is to assist all CMA supervised financial institutions in the Kingdom of Saudi Arabia in understanding and complying with their AML/CFT/CPF obligations relating to conducting a Business Risk Assessment pursuant to Article 5 of the Anti-Money Laundering Law issued by Royal Decree No. (M.20) dated 05/02/1439H, Article 63 of the Law on Combatting Terrorism Crimes issue by decree No (M/21) dated 12/02/1439H and Financing, Implementing Regulations, Rules and Guides.

2. This Guideline sets out the expectations of CMA regarding the factors that supervised financial institutions should take into account when conducting their Business Risk Assessment. CMA's expectations are in line with national AML/CFT/CPF obligations, FATF standards and international best practice.

3. The factors and measures described in this Guideline are not exhaustive and this Guideline does not set limitations on the steps to be taken by financial institutions in order to meet their statutory obligations.

4. There is no standard risk assessment methodology and in conducting their risk assessment, financial institutions should consider any other factors and measures as appropriate to their business.

5. This Guideline applies to all financial institutions which are subject to AML/CFT supervision by CMA.

Supervisory Expectations

6. Conducting a Business Risk Assessment (BRA) is a fundamental component of the Risk-Based Approach (RBA) mandated under the Financial Action Task Force (FATF) Recommendations. Financial institutions (FIs) are required to systematically evaluate the money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks associated with their business activities, customer base, products, services, and geographic exposure. This assessment enables FIs to identify, measure, and understand the inherent and residual risks they face. In this regard, FI's should also consider the relevant FATF guidance related to the Financial Sector.

7. **A BRA is the first step** FIs should take before developing their AML/CFT/CPF programmes. It involves identifying and assessing the inherent risks which FIs reasonably expect to face from ML/TF/PF. Once an FI has completed its' risk assessment, the entity can then put in place a programme that minimizes or mitigates these risks.

8. Having a **well-documented** ML/TF/PF risk assessment in place is a central part of an FI meeting its AML/CFT/CPF obligations and should assist financial institutions to:

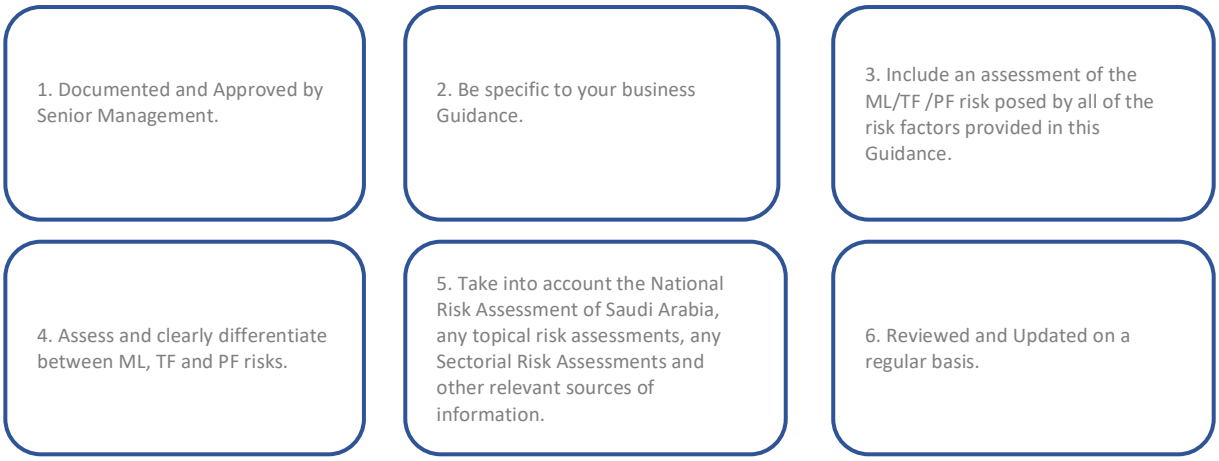
   a. Understand the ML/TF/PF risks to which the entire business is exposed,
   b. Determine how these risks are effectively mitigated through internal policies, procedures and controls and;
   c. Establish the residual ML/TF/PF risks and any gaps in controls that should be addressed.

9. FIs must ensure that their **BRA is tailored to their business** profile and takes account of the factors and risks specific to their business. A generic ML/TF/PF BRA that has not been adapted to the specific needs or business model of the supervised entity will not meet the expectations of CMA.

10. The BRA must be **made available** to CMA upon request.

11. FIs should note that **ML/TF/PF risk cannot be entirely eliminated** regardless of how effective the AML/CFT/CPF control framework is.

12. CMA expects that the BRA should satisfy all of the criteria provided below;



Overview of Business Risk Assessment

13. The primary objective of a BRA for an FI is to systematically identify, evaluate, and understand the risks associated with its operations, products, services, customers, and geographic exposure. This process enables the entity to assess the likelihood and impact of ML/TF/PF and other financial crime risks. By conducting a thorough risk assessment, the FI can develop and implement appropriate risk mitigation measures, ensuring compliance with regulatory requirements while safeguarding its integrity and reputation. Additionally, the BRA supports informed decision-making, enhances risk management frameworks, and promotes a proactive approach to financial crime prevention.

14. A BRA should not be confused with a Customer Risk Assessment. The **BRA identifies the risk of ML/TF/PF posed to the FI as a whole based on its activities**. A customer risk assessment specifically identifies the risks that each individual customer (individual or legal person) poses to the business.

15. The BRA consists of number of phases that should be conducted by an FI. The results of an effective ML/TF/PF BRA will be the classification of identified risks into different categories, such as High, Medium and Low or some combination of those categories (such as medium-high, medium-low etc).

16. An effective ML/TF/PF BRA will allow the FI to make informed management decisions regarding risk appetite, allocation of AML/CFT resources and development of ML/TF/PF risk mitigation strategies. Where higher risks are identified, FIs must take enhanced measures to mitigate these risks.

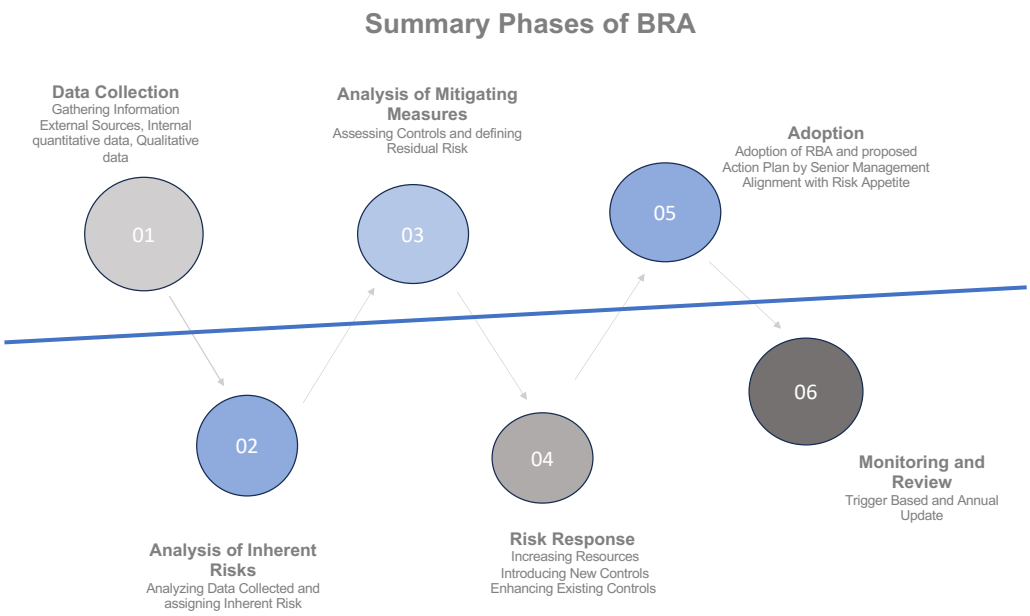
17. The risk that remains after all measures have been implemented effectively is known as the **residual risk.**

18. The FI must ensure that it properly documents and demonstrates the methodology used to determine residual risk ratings.

19. The BRA is a cyclical process and the **risk assessment should remain under regular review,** including whenever there are major developments in management and operations of the FI (e.g. business model, clientele, risk exposure, etc.). Supervised entities should also develop a list of trigger events that trigger an ad hoc review of the BRA.

Phases of a Business Risk Assessment

20. There are **6 main phases** of a BRA;



Phase 1: Data Collection

21. As part of the risk assessment process, an FI must evaluate its **inherent risks**, which represent the ML/TF/PF risks that exist before any controls or mitigation measures are applied.

22. When supervised entities are conducting their risk assessment, they should have regard to various **relevant sources of information.**

Examples include:

High-Level external sources on Risks	International Guidance, typologies and evaluations including the FATF, the Basel Committee, the World Bank, International Monetary Fund, United Nations and Transparency International
	Information from professional sectorial bodies
	Black lists, grey lists, sanctions lists
	Topical risk assessments conducted by Authorities in Saudi Arabia
	Saudi Arabia National Risk Assessment
	Risk Assessments conducted by supervisory authorities and other competent authorities, including SAFIU
	ML/TF Risks as issued by the Anti-Money Laundering Permanent Committee (AMLPC) and the Permanent Counter Terrorism Committee (PCTC)
	NRAs of other regions with links to the business
	Communications and guidance by competent authorities
	Guidance published by CMA
Operational Internal sources	Data on customers: numbers, types and locations
	Data on beneficial ownership of customers
	Results of analyses of unusual and suspicious transactions
	Findings of internal or external auditors
	Volume of transactions
	Proportion of cash transactions
	Product range and characteristics
	Reports from compliance
	Exposure to certain industries/sectors
	Size of the company
	Use of third parties
	Extent of non-face to face business

Stage 2: Inherent Risk Analysis[1]

23. FIs should analyze both quantitative and qualitative data when assessing inherent risk factors as part of the BRA. FIs should consider the following key risk categories:

a. **Structural Risk** – Risks arising from the entity's ownership structure, governance framework, and operational complexity, which may impact its vulnerability to financial crime.

[1] Examples of data relating to Inherent Risk is included in the individual annexes for SAMA, CMA and IA.

b. **Customer Risk** – The level of risk posed by the entity's customer base, considering factors such as customer type, industry, legal structure, transactional behavior, and potential exposure to high-risk individuals or entities.
c. **Products, Services, and Transaction Risk** – Risks associated with the nature of the products and services offered, as well as the complexity, volume, and frequency of transactions, which may create opportunities for illicit financial activities.
d. **Delivery Channel Risk** – The risk posed by the methods used to deliver products and services, including the extent to which digital, non-face-to-face, or third-party channels are utilized, which may increase anonymity and reduce oversight.
e. **Geographic Risk** – Risks linked to the jurisdictions in which the FI operates, conducts transactions, or has business relationships, particularly in regions with weak AML/CFT frameworks, high corruption levels, or significant exposure to financial crime.
f. **New and Existing Technologies Risk** – The risks associated with the adoption and use of emerging and existing technologies, including digital assets, fintech solutions, and automated systems, which may introduce new vulnerabilities or enhance illicit financial flows. The FI must assess such risks before launching any new products, services or business practices and before using new technologies or technologies under development.
g. **Emerging ML and TF/PF Risk** – FIs must ensure that they have systems and controls in place to identify and assess emerging ML and TF/PF risks, as well as existing risks that have increased in severity. These risks should be incorporated into the BRA in a timely manner. Key measures to manage emerging risks include:
    i. Regular review of internal data to identify trends and emerging financial crime threats.
    ii. Ongoing monitoring of external sources of information (e.g., regulatory updates, typologies, and intelligence reports).
    iii. Processes to assess and incorporate risks associated with new products and technologies.

24. Risk can be defined in various ways, and there is **no universally applicable assessment model for evaluating it.** Once an FI has identified the ML/TF/PF risks it faces in the course of its business activities, it must assess the level of those risks.

25. The BRA should also consider both current operational risks and those that are likely to emerge in the near future. This includes evaluating the potential impact of new products, services, customer segments, and technological advancements before such products and or technologies are launched. Furthermore, ML/TF/PF risks often interact and may present a heightened level of risk when combined.

26. There are multiple approaches to assessing risk, including but not limited to:

a. Evaluating the likelihood of an event occurring,
b. Assessing both the likelihood and potential consequences of an event,
c. Considering the interplay of vulnerability, threat, and impact,
d. Analyzing the effect of uncertainty on an event.

27. Regardless of the chosen method, the FI must be able to clearly explain and demonstrate its adequacy and effectiveness to its AML/CFT supervisor, ensuring that it is appropriate and proportionate to the FIs specific needs.

28. The risk assessment process should be well-informed, logical, and thoroughly documented. The BRA should explicitly outline the basis and evidence for this determination, referencing sources such as domestic regulatory guidance, case studies, direct business experience and any other relevant information.

Weighting of Risk Factors

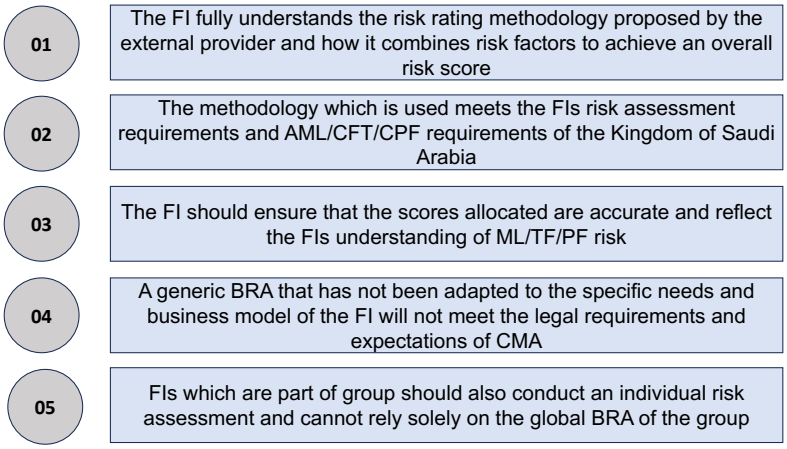
29. When assessing ML/TF/PF risk, FIs may decide to **weight risk factors** differently depending on their relative importance. FIs should consider the relevance of different risk factors in the context of a business relationship or transaction. The weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one FI to another.

30. FIs should chose a methodology, select a risk-rating scale and set parameters for risk ratings and weightings.

31. When weighting risk, FIs should ensure the following:

01	Weighting is not unduly influenced by just one factor
02	Economic or profit considerations do not influence the risk rating
03	Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk
04	Situations identified by the AML/CFT Legislation as always presenting a high ML/TF/PF risk cannot be overruled by the FIs weighting
05	FIs can override any automatically generated risk score where necessary. The rationale for the decision to override such scores should be governed and documented appropriately.

32. Where FIs use **automated IT systems** to allocate overall risk scores to categorize business relationships or transactions and do not develop these inhouse but rather purchase them from an external provider, they should ensure the following:



Phase 3: Analysis of Risk Mitigation Measures

33. **Risk mitigation** involves assessing the adequacy and effectiveness of the risk mitigation measures (controls) implemented within the business.

34. FIs should ensure that they have **appropriate policies, procedures and controls** in place to effectively manage and mitigate the ML/TF/PF risks which they have identified, including the risks which have been identified at a national level. The policies, procedures and controls should be approved by senior management. They should be appropriate and proportionate to the risks identified and should be subject to ongoing monitoring and review to ensure that they continue to effectively manage and mitigate the level of risk identified.

35. The level of inherent ML/TF/PF risk directly influences the nature and intensity of these controls, as well as the allocation of AML/CFT resources.

Examples of effective risk mitigation measures include;

Customer due diligence measures to verify customer identities and assess risk profiles.

Record-Keeping and reporting measures to ensure compliance with regulatory obligations.

Risk Management and internal controls including;

- Client acceptance policies.
- Procedures for customer risk assessment.
- Compliance frameworks.
- Independent testing of car
- Customer Screening.
- Transaction Monitoring Process.
- Standards for hiring & training employees.

36. The effectiveness of these controls depends on their consistent implementation in daily operations. Therefore, FIs must conduct ongoing monitoring to ensure their proper application, evaluate their effectiveness, and promptly address any deficiencies or gaps.

37. An assessment of the **level and adequacy** of the controls which are in place includes:

a. The level of inherent ML/TF risk influence the type and levels of AML/CFT controls and resources,
b. Controls and risk mitigation strategies which are required to be put in place
c. Whether the control is automatic or manual
d. Whether the internal audit/external audit has tested it (Controls regularly tested with positive results)
e. Whether it is a primary or secondary control
f. Whether it has been implemented for more than 1 year
g. Whether is a preventive or detective type of control

38. For the purpose of this guidance preventive controls are those that limit the ability to use the product or channel in a way that would increase the ML/TF/PF risks. This includes controls related to setting transaction limits or having a management approval process for high-risk customers, products, or countries, applying EDD measures with specific customers. Detective controls only seek to monitor activity through the product or channel. This would be information related how the product or channels are used, and information related to transaction monitoring and suspicious transaction reporting.

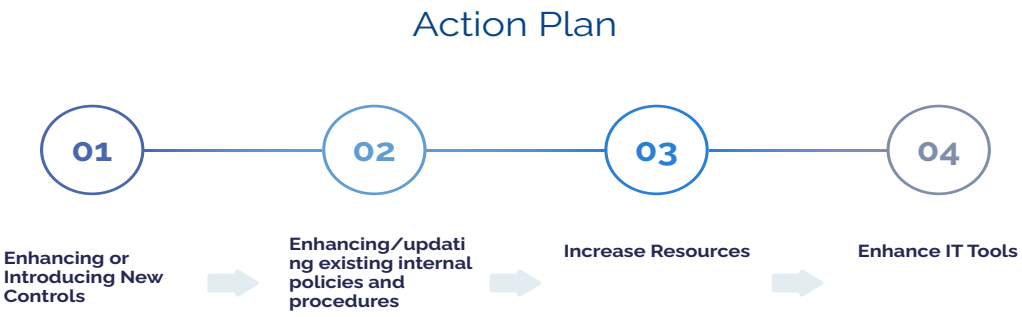
Phase 4: Risk Response

39. The previous phases should ultimately lead to the determination of **residual risk,** which refers to the risks that remain after the implementation of risk mitigation measures and internal controls. Regardless of how effective the control framework is, it is important to note that ML/TF/PF risk can never be completely eliminated. Certain risks will always remain due to external factors, evolving threats, and limitations in control mechanisms.

40. In this phase, the FI must evaluate whether the residual risks it faces align with its risk appetite, which defines the level of risk the institution is prepared to accept in the course of its business operations. This assessment ensures that the FI is not operating beyond its risk tolerance and that necessary adjustments can be made to strengthen controls where required.

41. Following the identification and assessment of inherent risks and the corresponding risk mitigation measures, the FI should develop a **comprehensive Action Plan**. This plan should outline specific steps to address any gaps in controls, enhance risk management processes, and reinforce compliance measures where residual risks exceed acceptable thresholds.

42. The Action Plan should be regularly reviewed and updated to ensure that emerging risks are promptly identified and effectively managed within the institution's overall AML/CFT/CPF framework.



Phase 5: Adoption

43. The BRA and Action Plan should be **documented and adopted** by the senior management of the supervised entity.

44. It is also important that **employees are made aware of the results** of BRA, for example through the ongoing employee ML/TF/PF training programme. This ensures that employees are aware of the main risks that the entity is exposed to and that they can effectively execute the policies, procedures and controls determined by senior management to mitigate the risks.

Phase 6: Monitoring and Review of the BRA

45. As ML/TF/PF risks are always changing, the ML/TF/PF risk assessment should be subject to continual review. Where an FI is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible. FIs should also assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

46. FIs should ensure that they have systems and controls in place to ensure that their risk assessment remains up to date. For example, setting a timeline as to when the next BRA will take place to ensure changing, new or emerging risks are included. **FIs are expected to review the BRA on an on-going basis.** The updates should include the following:

- Updated quantitative and qualitative information;
- New insights from National and/or Sectorial Risk Assessments;
- Review of risks related to product, services, delivery channels;
- Regulatory updates.
- Any updates related to the region.

47. In addition, FIs should also develop an internal list of **trigger events** which may also give rise to an ad hoc review of the BRA. Examples of events which might trigger a review of the BRA include:

- New products, services or delivery channels
- Implementation of new technologies
- Change in clientele
- Significant regulatory changes
- Significant increase in risk
- New corporate structure
- Change in business model

48. Any update to the BRA, just like the original risk assessment, must be documented, and commensurate to the ML/TF/PF risk.

49. FIs should recognize that BRA is not merely a compliance exercise or a one-time documentation requirement. Instead, it should serve as a dynamic and integral component of the institution's risk management framework, guiding decision-making and operational practices.

Annex

Investment Companies and Investment Brokers

Overview of Inherent Risk Factors

50. There are a number of key characteristics and vulnerabilities of the capital markets/securities sector which capital markets institutions should consider when conducting a BRA. These include:

- Possibilities to conduct high level of transactions, with a high speed and a global reach across a multitude of onshore/offshore jurisdictions;
- Easy access to many different markets (both on registered securities exchanges and elsewhere, e.g. over-the-counter markets and electronic trading platforms);
- Common involvement of a multitude of participants on behalf of both buying and selling parties, which can limit abilities to have complete oversight of the transaction;
- Complex customer corporate structures;
- Complexity of products;
- Abilities to transact in securities products via intermediaries which may provide a relative degree of anonymity to underlying investors/customers;
- The diverse roles that providers and intermediaries play in transactions, for example acting as investment fund manager and depository bank;
- Abilities to transact in complex, not yet regulated products;
- High liquidity of some products, enabling their easy conversion to cash;
- Pricing volatility of some products, particularly low-priced securities, and challenges in pricing some securities products due to their bespoke nature or complexity.

51. Vulnerabilities in this sector are seen in the layering and integration phase of money laundering, once criminals or their facilitators have found a way to insert illicit cash into the financial market and then further disguise its criminal origins. Capital markets are characterized by high-speed, global transactions with fragmented oversight which allows for many layers to be built in a short period of time and relatively easy manner between the illicit origins of funds and their final investment or use.

52. The incorporation of virtual assets (VAs) into investment portfolios also raises the level of risk that those entities are exposed to, due to their speed of transfer, global reach and anonymity.

53. As regards **customer** risk, those capital market institutions that have customers which are charitable or other non-profit organizations (NPOs) linked to high-risk areas or conflict zones, or customers who donate the securities that they have purchased to such NPOs pose higher risks from a customer risk perspective. In addition, crowdfunding activities and web-based funding

activities involving virtual assets which may in some contexts be linked to the capital markets industry, are generally believed to pose higher TF risks.

54. Regarding **delivery channels**, intermediation is very common in this sector. It is a general feature of many transactions in capital markets, especially secondary markets, to involve a large number of firms using each other's products or services for their own underlying customers whereby a single firm can generally only see their own direct customer. There is also a practice of FIs acting as intermediaries or introducers for each other's business. Intermediation can expose CMIs to heightened ML/TF/PF risks, with specific risks varying based on the activity that intermediaries undertake and their relationship with the company.

55. The use of non-face to face delivery channels including the possibilities to open accounts online and tools which allow automatic customer verification also attracts a higher risk of ML/TF/PF.

Table: Examples of the Data that should be collected by Investment Companies and Investment Brokers for each risk factor and examples of quantitative information

Structural Risk Factors	
Nature of the business	Annual turnover
Size/scale of the business	Annual net profit
Diversity and complexity of business lines	Number of employees
Diversity and complexity of markets in which the company operates	Number of branches or offices
Number of different business lines	Number of markets in which the company operates
Total value of assets under management	

Customer Risk Factors	
Total number of customers	Legal person customers with nominee shareholders or nominee directors
Type of customer (natural persons, legal persons, legal arrangements)	Persons acting as representatives/nominees on behalf of the customer
Non-resident customers	Other high-risk businesses and links to sectors which are commonly associated with higher level of ML/TF risk
PEP customers (foreign, domestic, international organizations; customers and BOs of customers)	Customers with complex ownership structures
High net worth individuals	Holders of bearer shares or other bearer negotiable instruments

Cash intensive business	Number of customers (individuals, legal persons and legal arrangements in the categories mentioned
Special Purpose Vehicles	Total number of transactions
NPOs	Total value of transactions
	Total number of deposits, assets,

Product/services/transaction risk factors	
Level of transparency of the product, service or transaction and extent that the product, service or transaction might facilitate or allow anonymity or opaqueness of the customer, ownership or beneficiary structures	Number of customers (natural person, legal person, legal arrangement) per product/service
Products or services that allow the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party.	Transaction value per product/service
Products that have been subject to fraud and market abuse such as low-priced securities/penny stocks.	Number of products issued
The purchase of securities using physical cash.	Number of transactions per each payment means
Offering bank like products such as check cashing and automated withdrawal cards	Volume of funds transferred per each payment means;
Securities-related products or services funded by payments from or instruction given by unexpected third parties, particularly from higher risk jurisdictions	Number and volume of cross-border transfers
Transactions involving penny/microcap stocks	Profile of customers that use particular payment means
Complex or unregulated products	High Liquidity Products
Products subject to volatile pricing	

Delivery Channels	
Non-face to face onboarding	Number of business relationships that have been entered into face to face
Use of introducers, intermediaries and/or agents	Number of business relationships that have been entered into non- face to face
Reliance on third parties for CDD	Number of customers (natural persons, legal persons and legal arrangements) onboarded through each delivery channel
New and untested delivery channels	Number of introducers, intermediaries and/or agents

Introducers, intermediaries and/or agents geographies	Third parties' geographies
	Profile of the customers that came through each delivery channel

Geographic Risk Factors	
Countries subject to sanctions – TF and PF	Country breakdowns for - Customers (natural persons, legal persons and legal arrangements) - Beneficial owners of customers - Transactions (incoming and outgoing) - Products and services - Introducers, agents, intermediaries etc.
FATF blacklisted/grey-listed countries	
Offshore jurisdictions	
Tax non-compliant jurisdictions	
Countries associated with high level of corruption or organized crime	

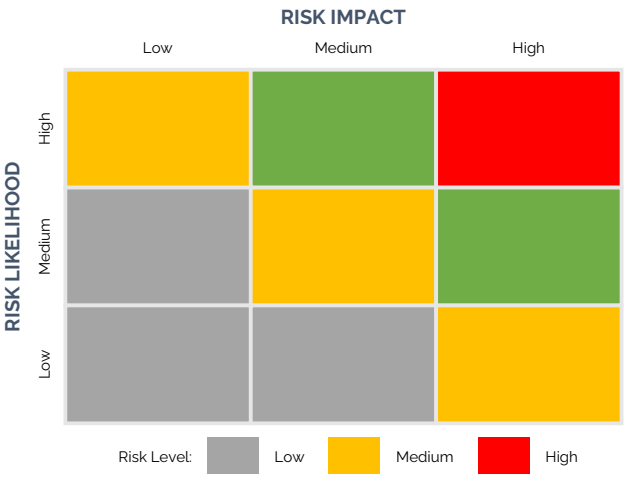
Risk Mitigation

Examples of information on controls to be considered in BRA:

1. Since when has the control been implemented
2. Dedicated resources to implement the control
3. Training Provided to persons implementing the control
4. Level of oversight on the application of the control
5. Whether the control has been subject to independent testing
6. Budget for EDD on high-risk clients, eg obtaining external intelligence
7. Availability of reliable data on domestic and foreign beneficial owners
8. Frequency of CDD reviews
9. Automatic versus manual controls
10. Periodic screening of whole database
11. Commercial databases used for sanctions & PEP screening
12. Responsibilities and timeframes for updating of sanctions lists

Risk Assessment - Example

#	RISK DESCRIPTION	CONTROLS /RISK MITIGATION
1	Risk of processing transactions for a person subject to Targeted Financial Sanctions List	❑ CDD/EDD Process and tools ❑ Screening of Customers in Sanctions Lists ❑ Identification and verification of BO
2	Risk of processing illegal funds for HNWI	❑ CDD/EDD Process ❑ Source of Funds and Source of Wealth Information ❑ Transaction Control – requested additional documents
3	Risk of onboarding customers subject to ML/TF investigation	❑ CDD Process ❑ Screening for Negative Media ❑ Period screening of customer base



هيئة السوق المالية
Capital Market Authority

Thank You