اللجنة الوطنية لمكافحة
غسل الأموال وتمويل الإرهاب
NATIONAL COMMITTEE
FOR AML & CFT

SUPERVISORY GUIDANCE ON
BUSINESS RISK ASSESSMENT

June 2025

Email: ncamlcft@kwfiu.gov.kw

Index

1. Purpose and Scope 4
2. Supervisory Expectations 4
3. Overview of Business-Wide Risk Assessment 6
4. Data Collection and Inherent Risk Analysis 7
5. Risk Mitigation 10
6. Risk Response 11
7. Approval and communication of the BRA 12
8. Review and updating of the BRA 12

1. Purpose and Scope

1. The purpose of this Guideline is to assist financial institutions in understanding and complying with their AML/CFT obligations relating to conducting a Business Wide Risk Assessment pursuant to Article (4) of the Law 106 and Article (1) of CBK Instructions, Article (2-3) from CMA's 16th Book of Executive Regulations and Article (8) of IRU Regulations.
2. This guidance is jointly developed by Central Bank of Kuwait, Capital Markets Authority, and Insurance Regulatory Unit.
3. This Guideline sets out the expectations of Supervisory Authorities regarding the factors that financial institutions should take into account when conducting their business risk assessment. 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. There is no standard risk assessment methodology and in conducting their risk assessment, supervised entities should consider any other factors and measures as appropriate to their business.
4. This Guideline applies to all financial institutions which are subject to AML/CFT supervision by CBK, CMA, and IRU.

2. Supervisory Expectations

5. 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 consider the FATF guidance related to the Financial Sector.

FATF Guidance on implementing the RBA for FIs

FATF
GUIDANCE FOR A RISK-BASED APPROACH
THE BANKING SECTOR
OCTOBER 2014
FATF
GUIDANCE FOR A RISK-BASED APPROACH
MONEY OR VALUE TRANSFER SERVICES
FEBRUARY 2016
FATF
GUIDANCE FOR A RISK-BASED APPROACH
SECURITIES SECTOR
OCTOBER 2018
FATF
GUIDANCE FOR A RISK-BASED APPROACH
LIFE INSURANCE SECTOR
OCTOBER 2018
LIFE INSURANCE

6. A Business Wide risk assessment is the first step supervised entities take before developing AML/CFT program. It involves identifying and assessing the inherent risks financial institution reasonably expects to face from ML/TF. Once supervised entity completes risk assessment, the entity can then put in place a program that minimizes or mitigates these risks. Having a well-documented ML/TF risk assessment in place is central for supervised entity to meet its AML/CFT obligations and should assist financial institutions in:

   a. understanding the ML and TF risks to which the entire business is exposed,

   b. determining how these risks are effectively mitigated through internal policies, procedures and controls and

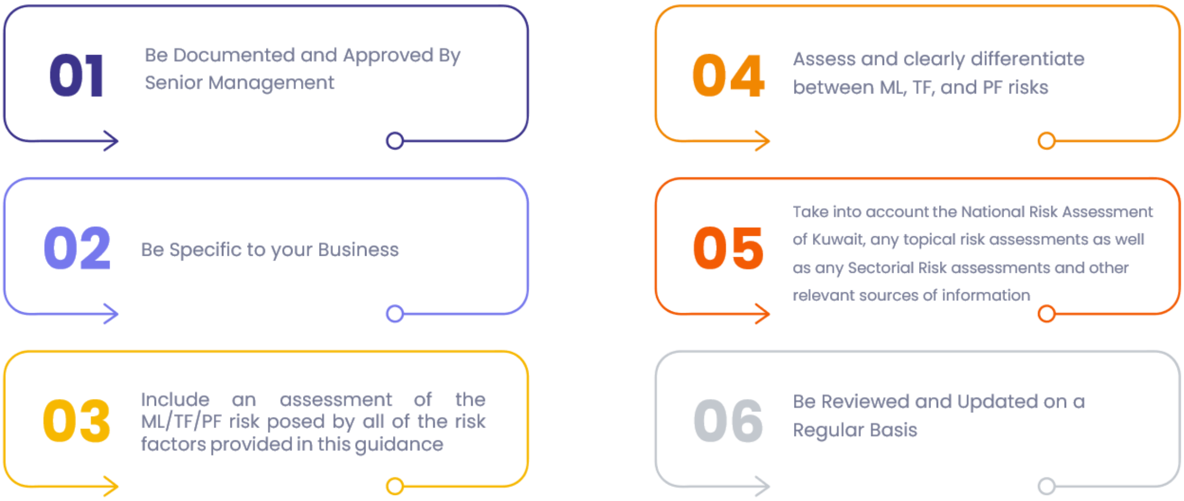
   c. establishing the residual ML/TF risks and any gaps in controls that should be addressed.

7. Supervised Entities 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 business risk assessment that has not been adapted to the specific needs or business model of the supervised entity will not meet the expectations of Supervisory Authorities.

8. Supervised entities should note that ML/TF/PF risk cannot be entirely eliminated regardless of how effective the AML/CFT control framework is.

9. Supervised entities keep in mind that an effective AML/CFT regime is risk-based. AML/CFT Compliance Program must manage and mitigate the ML/TF risks faced by the supervised entity.

10. Supervisory Authorities expect that the Business Risk Assessment Should satisfy the criteria provided below.



01 Be Documented and Approved By Senior Management

02 Be Specific to your Business

03 Include an assessment of the ML/TF/PF risk posed by all of the risk factors provided in this guidance

04 Assess and clearly differentiate between ML, TF, and PF risks

05 Take into account the National Risk Assessment of Kuwait, any topical risk assessments as well as any Sectorial Risk assessments and other relevant sources of information

06 Be Reviewed and Updated on a Regular Basis

3. Overview of Business-Wide Risk Assessment

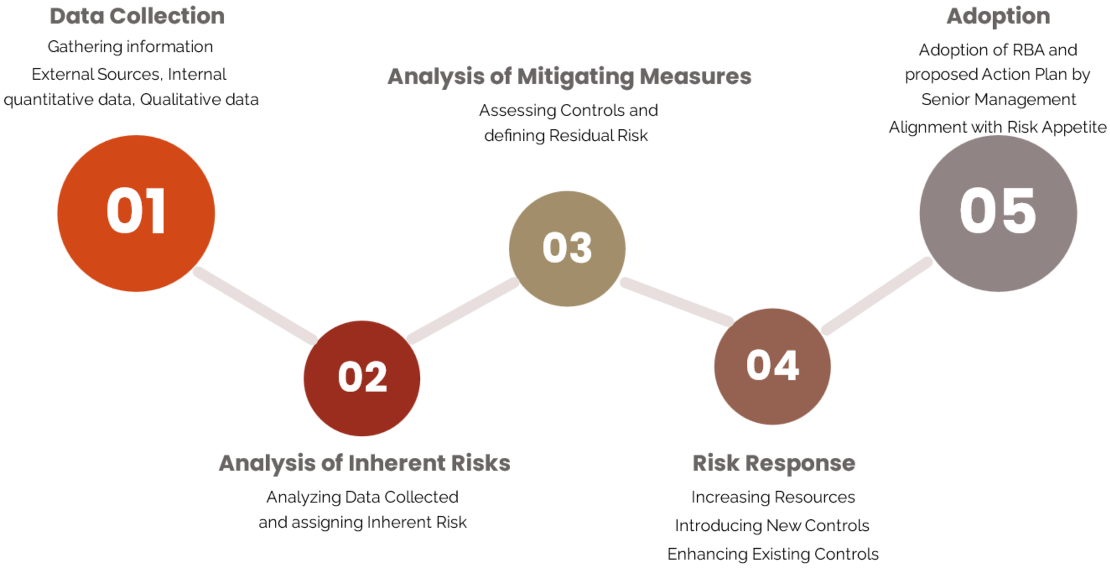
11. The primary objective of a Business Risk Assessment (BRA) for a supervised entity is to systematically identify, evaluate, and understand the risks associated with its operations, products, services, customers, and geographic exposure. This process enables the entity to assess the likelihood and impact of money laundering (ML), terrorism financing (TF), proliferation financing (PF), and other financial crime risks. By conducting a thorough risk assessment, the entity 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.

12. The Business Wide Risk Assessments consists of number of phases that should be conducted. The results of an effective ML/TF 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).

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

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

Summary of Phases of BRA



15. A common method of misuse is the utilization of legal persons and arrangements to conceal ownership and control rights. By creating a legal entity or legal arrangement, a criminal can create a layer of distance between himself and his/her illicit assets to complicate their detection and hinder any criminal investigations. While many companies are legitimate, the outlined scenario can be exploited to evade tax obligations, conceal illicit funds, and to facilitate money laundering.

4. Data Collection and Inherent Risk Analysis

16. As part of the risk assessment process, a supervised entity must evaluate its inherent risks, which represent the money laundering (ML) and terrorism financing (TF) risks that exist before any controls or mitigation measures are applied. The supervised entity must ensure that it properly documents and demonstrates the methodology used to determine residual risk ratings.

17. 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 risk

- International guidance, typologies & evaluations
- Information from professional sectorial bodies
- Black lists, grey lists, sanctions lists
- Topical risk assessments conducted by Authorities in Kuwait
- Kuwait National Risk Assessment
- Sectorial risk assessments conducted by CBK, CMA, IRU
- NRAs of other regions with links to the business
- Communications by competent authorities
- Guidance published by CBK, CMA, IRU

Operational Internal Sources - Examples

Data on customers: numbers, types, locations	Data on beneficial ownership of customers	Results of analysis of unusual & 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

18. Financial institutions should analyze quantitative and qualitative data When assessing inherent risk factors as part of a Money ML/TF/PF. Financial institutions 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.

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 entity 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.

g. Emerging ML and TF/PF Risk – Supervised entities 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.

Examples of the data that should be collected for each risk factor and examples of quantitative information	
Structural Risk Factors	
Nature of the business	
Size/scale of the business	Number of employees
Diversity and complexity of business lines	Number of branches or offices
Diversity and complexity of markets in which the company operates	Number of markets in which the company operates
Annual turnover	Number of different business lines
Annual net profit	Total Assets, overall and per business line/market

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

Product/Services/Transaction Risk Factors	
Complexity of the product, service or transaction 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 Cash services Deposits Wire transfers Private banking/wealth management Credit cards Prepaid cards	Trade finance transactions Means of payments: Cash, Checks, Prepaid cards, Virtual currency, etc. Number of products issued Number of customers (natural person, legal person, legal arrangement) per product/service Transaction value per product/service Number of transactions per each payment means Volume of funds transferred per each payment means; Profile of customers that use particular payment means

Delivery Channel risk factors	
Direct onboarding of customer Non-face to face onboarding of customer Internet banking Mobile banking Use of introducers, intermediaries and/or agents Reliance on third parties for CDD New and untested delivery channels Number of business relationships that have been entered into face to face Number of business relationships that have been entered into non- face to face	Number of customers (natural persons, legal persons and legal arrangements) onboarded through each delivery channel 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 FATF blacklisted/grey-listed countries Offshore jurisdictions Tax non-compliant jurisdictions Countries associated with high level of corruption or organized crime	Country breakdowns for - Customers (natural persons, legal persons and legal arrangements) - Beneficial owners of customers - Transactions (incoming and outgoing) - Products and services - Trade finance - Introducers, agents, etc.

19. Risk can be defined in various ways, and there is no universally applicable assessment model for evaluating it. Once a supervised entity has identified the money laundering (ML) and terrorism financing (TF) risks it faces in the course of its business activities, it must assess the level of those risks.

20. The risk assessment 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. Furthermore, ML/TF risks often interact and may present a heightened level of risk when combined.

21. 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.

22. Regardless of the chosen method, the supervised entity 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 institution's specific needs.

23. The risk assessment process should be well-informed, logical, and thoroughly documented. The risk assessment should explicitly outline the basis for this determination, referencing sources such as domestic regulatory guidance, case studies, or direct business experience.

24. When assessing ML/TF risk, supervised entities may decide to weight risk factors differently depending on their relative importance. Supervised entities 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 supervised entity to another. When weighting risk, supervised entities should ensure the following:

1. Weighting is not unduly influenced by just one factor;
2. Economic or profit considerations do not influence the risk rating;
3. Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
4. Situations identified by the AML/CFT legislation as always presenting a high ML or TF risk, cannot be overruled by the supervised entity's weighting;
5. Supervised entities can override any automatically generated risk score where necessary. The rationale for the decision to override such scores should be governed and documented appropriately.

25. Where supervised entities 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 that: To prevent misuse of Kuwaiti legal entities and legal arrangements, a number of obligations exist with regards to beneficial ownership, which can be broadly categorized into three types:

1. The supervised entity fully understands the risk rating methodology proposed by the external provider and how it combines risk factors to achieve an overall risk score;
2. The methodology which is used meets the entity's risk assessment requirements and AML/CFT requirements of Kuwait.
3. Supervised entity should ensure that the scores allocated are accurate and reflect the entity's understanding of ML/TF risk.

5. Risk Mitigation

26. Risk mitigation involves assessing the adequacy and effectiveness of the risk mitigation measures implemented within the business.

27. Supervised entities should ensure that they have appropriate policies, procedures and controls in place to effectively manage and mitigate the ML/TF 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.

28. Supervised entities must establish and maintain comprehensive policies, controls, and procedures designed to prevent identified risks from materializing or to mitigate their impact. The level of inherent money laundering (ML) and terrorism financing (TF) risk directly influences the nature and intensity of these controls, as well as the allocation of AML/CFT resources. Effective risk mitigation measures should encompass for example:

- Customer due diligence (CDD) 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 controls,
    - Customer Screening,
    - Transaction Monitoring Process,
    - Standards for hiring and training employees, among others.

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

30. An assessment of the level and adequacy of the controls which are in place noting the following:

a. the level of inherent ML/TF risk influence the type and levels of AML/CFT 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 it is a preventive or detective type of control

31. 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 to how the product or channels are used, and information related to transaction monitoring and suspicious transaction reporting.

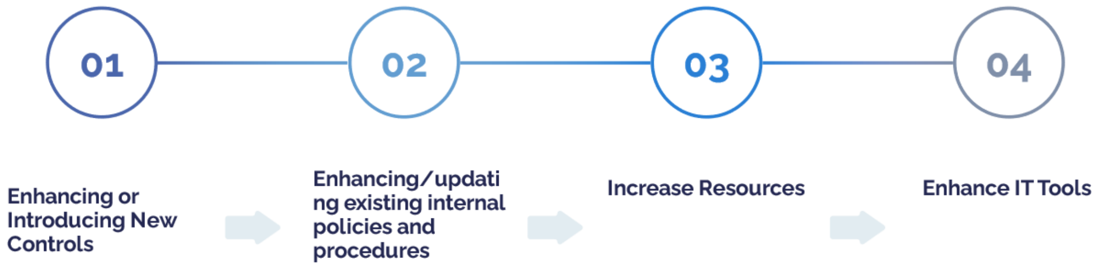
6. Risk Response

32. The previous two phases should ultimately lead to the determination of residual risk, which refers to the risks that persist even after the implementation of risk mitigation measures and internal controls. While FIs strive to mitigate money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks through robust compliance frameworks, it is important to acknowledge that these risks can never be completely eradicated. Regardless of how well-designed and effective a control framework may be, certain risks will always remain due to external factors, evolving threats, and limitations in control mechanisms.

33. 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 institution is not operating beyond its risk tolerance and that necessary adjustments can be made to strengthen controls where required.

34. 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. 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 framework.

Action Plan


01
02
03
04
Enhancing or Introducing New Controls
Enhancing/updating existing internal policies and procedures
Increase Resources
Enhance IT Tools

7. Approval and communication of the BRA

35. The BRA should be documented and adopted by the senior management of the supervised entity.

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

8. Review and updating of the BRA

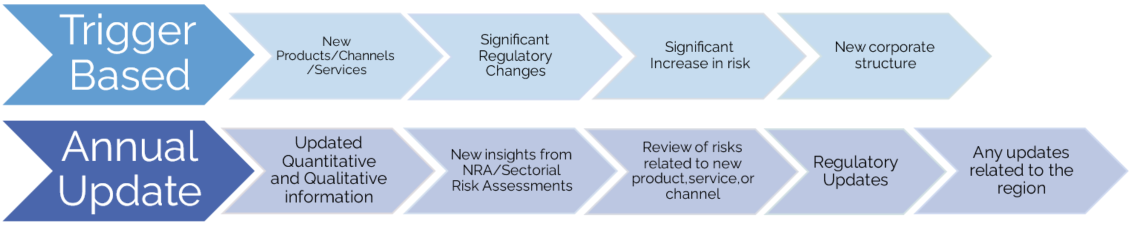
37. As ML/TF/PF risks are always changing, the supervised entity should reassess its exposure to ML/TF/PF risks accordingly and in a timely manner. Where a supervised entity is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible. Supervised entities should also assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

38. Supervised entities 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. Also, it's important that entities develop list of trigger events when the update will be conducted. Any update to the BRA, just like the original risk assessment, must be documented, and commensurate to the ML/TF risk.

39. Financial institutions 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.

40. FIs are expected to conduct update annually but also to consider updating BRA based on trigger events.

Monitoring and Update of BRA


Trigger Based
New Products/Channels /Services
Significant Regulatory Changes
Significant Increase in risk
New corporate structure
Annual Update
Updated Quantitative and Qualitative information
New insights from NRA/Sectorial Risk Assessments
Review of risks related to new product,service,or channel
Regulatory Updates
Any updates related to the region