مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

BEST PRACTICES FOR LICENSED FINANCIAL INSTITUTIONS ON IMPLEMENTING A RISK-BASED APPROACH AND CONDUCTING RISK-BASED INSTITUTIONAL RISK ASSESSMENTS

03 September 2025

CentralBankUAE
CentralBankUAE
Central Bank of the UAE
CentralBankoftheUAE
Central Bank of the UAE
المصرف–المركزي.امارات
www.centralbank.ae
Central Bank of the UAE:
Download on the App Store
GET IT ON Google Play
المصرف-المركزي.امارات
www.centralbank.ae

AGENDA

1 Legal Basis

2 Implementing a Risk-Based Approach

3 Conducting Institutional Risk Assessment

4 Principles and Best Practices of an Institutional Risk Assessment

5 Application of the Risk-Based Approach

6 Next steps: Gap Analysis & Implementation

Purpose and Applicability of the Best Practice

Purpose

- This Best Practice does **NOT** constitute new regulation and does **NOT** introduce new legal obligations.
- It is designed to help CBUAE's LFIs understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.
- LFIs are expected to demonstrate compliance with requirements of this Best Practice within one month from its coming into effect.

Applicability

This Best Practice document applies to **all natural or legal persons that are licensed and/or supervised by the CBUAE** in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, investment companies, payment service providers, virtual asset service providers ("VASPs"), payment token service providers, registered hawala providers;; and
- Insurance companies, agencies and brokers.

Legal Basis

- **Federal Decree Law No. 20 of 2018** on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended (“AML-CFT Law”).

- **Cabinet Decision No. (10) of 2019** concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 (“AML-CFT Decision”) and its amendments.

- **Cabinet Decision No. (74) of 2020** Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution (“Cabinet Decision 74”), and its amendments.

- **Cabinet Resolution No. (50) of 2020** concerning the control list annexed to Federal Law No. 13 for 2007 relating to commodities subject to import and export control.

- **Federal Decree Law No. (43) of 2021** on the commodities subject to non-proliferation.

- Notice No.: **CBUAE/BIS/2023/5960**, which mandates all LFIs to take steps to identify, assess, understand, and mitigate PF risks on an institutional level.

Implementing a Risk-Based Approach

Implementing a Risk-Based Approach (1/2)

- The Risk-based approach ("RBA") requires LFIs to **identify**, **assess**, **understand**, and **manage** the ML/TF/PF risks they are exposed to, and subsequently **apply** AML/CFT/CPF measures commensurate with those risks in order to manage them effectively.
- A reasonably designed RBA will provide a framework for identifying the degree of potential ML/TF/PF risks associated with an LFI's **customers**, **products and services**, **delivery channels**, **geographic locations and markets**, and **operating structure,** and enable an institution to focus on those risk factors that pose the greatest ML/TF/PF risk.

As a **general principle**, where there are higher risks, LFIs should take enhanced measures to manage and mitigate the risks; where the risks are lower, simplified measures may be permitted.

Implementing a Risk-Based Approach (2/2)

- Under the RBA, institutions that face higher ML/TF/PF risks are expected to develop enhanced measures to mitigate such higher risk by expanding the range, degree, frequency, and intensity of their mitigating controls.
- Conversely, institutions that face lower ML/TF/PF risks may choose to implement simplified measures, provided these are consistent with minimum legal and regulatory obligations. Thus, an RBA consists of the following steps:

Assessing Risk: Institutional Risk Assessment

- Inherent Risk
- Mitigating Controls
- Residual Risk

Mitigating Risk: Application of RBA

- Risk Appetite Alignment
- Application of the risk-based approach when implementing the AML/CFT/CPF controls.

Conducting Institutional Risk Assessment

Institutional Risk Assessment

What is a Risk Assessment?

While the RBA is the overall framework and process used to manage ML/TF/PF risk, the conduct of the ML/TF/PF risk assessment is a key component of the RBA.

Risk assessment consists of:

a) identifying an institution's inherent ML/TF/PF risks based on the LFI's specific characteristics, business model, and activities;
b) reviewing the design and operational effectiveness of the LFI's control framework to manage these risks; and
c) determining the residual risk that remains after an LFI's controls are applied to its inherent risk.

Inherent Risk − **Mitigating Controls** = **Residual Risk**

Simpler risk assessments may be sufficient for smaller or less complex institutions that carry similar categories of customers or whose activities are circumscribed to a particular jurisdiction or service.

Conversely, complex institutions, which service a diverse pool of clients, provide different types of services, or operate in several jurisdictions, will need to perform risk assessments that are sophisticated and aligned with the LFI's complexity.

Institutional Risk Assessment – Benefits and Outcomes

- **Developing an accurate risk appetite statement** that adequately reflects an institution's ML/TF/PF risk tolerance and allows it to implement effective controls and allocate resources on the basis of risk.
- **Identifying gaps or opportunities for improvement** in AML/CFT/CPF policies, procedures, processes, systems, and other mitigating controls.
- **Understanding** how a business unit's AML/CFT/CPF compliance program aligns with its risk profile.
- Lowering an institution's residual risk exposure by **developing effective risk mitigation strategies** and/or reducing exposure to inherent risks that cannot be managed effectively.
- **Informing supervisors** about key risks, control gaps, and remediation efforts across the institution.
- **Assisting senior management** with strategic decisions in relation to customer exits and account restrictions.
- **Enhancing regulatory compliance and reporting**; ensuring that the institution meets all relevant AML/CFT/CPF requirements.
- **Ensuring senior management is informed** of the institution's key risks, controls gaps, and remediation efforts.

Attributes of an Effective Risk Assessment Methodology

- Risk assessment methodology should document all the steps of the risk assessment process and the rationale that supports the ML/TF/PF risk assessment, such as reasoning behind chosen risk factors, scoring criteria, and instances when the LFI has chosen to deviate from standard practices.
- Although there is no standard risk assessment methodology, the ML/TF/PF risk assessment methodology should describe the following factors:

  - Risk factors assessed;
  - Types of quantitative or qualitative data that is being evaluated;
  - Stakeholders involved in the development of the risk assessment;
  - Risk scoring criterion;
  - Assigning of weightings to risk factors; and
  - Risk scoring overrides, as applicable.

LFIs should integrate external sources of information, such as the UAE national risk assessment, sectoral risk assessments, industry reports, and feedback from supervisory authorities, to enhance the accuracy and relevance of the risk evaluation.

Institutional Risk Assessment

Granularity and level of detail in the risk assessment.

LFIs have flexibility regarding how they organize their ML/TF/PF risk assessments. Depending on the **size**, **entity type**, and **complexity** of the specific institution, a risk assessment may be organized across business lines or legal entities (referred to as assessment units) that can be consolidated into an enterprise-level risk assessment.

As much as is possible or practical, LFIs should consider adopting **standardized methodologies** across assessment units, while ensuring that assessment processes retain flexibility across disparate units to allow for a tailored assessment of risk.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Institutional Risk Assessment

Consultation, accountability and stakeholders relevant to the Risk Assessment.

Who manages and owns the risk assessment process will be influenced by the structure, global footprint, and complexity of an LFI.

With that understanding, the ML/TF/PF risk assessment process should be:

- **managed** by the LFI's Money Laundering Reporting Officer ("MLRO")/Compliance Officer, in coordination with the appropriate risk management function, and
- **owned** by the Board of Directors, shareholders and senior management.

Institutional Risk Assessment

Frequency of a ML/TF/PF Risk Assessment.

An LFI's ML/TF/PF risk assessment should be updated, at a minimum, on an **annual basis**, and also in response to certain "**trigger**" events.

Examples of trigger events:	
	Changes in the LFI's organizational structure, business model, or strategy, such as due to mergers or acquisitions and expansion into new markets. This may also include global and regional events with a significant bearing on the LFI's activities.
	Activities stemming from the LFI's customer base; introduction of new products, services, or technologies; or the jurisdictions where the LFI operates.
	AML/CFT/CPF program, including updates to applicable AML/CFT/CPF laws and regulations and implementation of new AML/CFT/CPF controls.
	The UAE's National ML/TF/PF Risk Assessment and CBUAE's Sectoral ML/TF/PF Risk Assessment.

Principles and Best Practices of an Institutional Risk Assessment

Fundamental Elements of an Institutional Risk Assessment

An institutional risk assessment consists of three core steps:

- **Inherent Risk**: an identification and assessment of the ML/TF/PF risks inherent to an LFI's business model and activities, including specific risks associated with an LFI's customers, products and services, delivery channels, geographies, and operating structure.
- **Assessing the Control Environment**: an assessment of the design and operational effectiveness of the policies, procedures, systems, and other controls in place to mitigate the LFI's inherent ML/TF/PF risks.
- **Residual Risk**: an assessment of the risk that remains after an LFI's controls are applied to its inherent risk.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

General Best Practices for Conducting a Risk Assessment

Whilst risk assessments will vary according to the LFI's activities and risk profile, all LFIs should implement the following best practices associated with their ML/TF/PF institutional risk assessments:

- **Data Quality**: LFIs should conduct thorough data quality checks using scientific methods or algorithms to address missing or incorrect data and utilize feedback mechanisms for inconsistencies.
- **Quantitative Calculations**: LFIs should use quantifiable metrics to inform the risk assessment, establishing criteria to measure AML/CFT/CPF control effectiveness.
- **Workpapers**: LFIs should maintain records of workpapers and tools used for data collection and scoring in the ML/TF/PF institutional risk assessment.
- **Report**: LFIs should prepare an enterprise-level risk assessment report, including assessments of inherent risks, mitigating controls, and residual risks, with supporting data and analysis.
- **Policies and Governance Documentation**: LFIs should document their risk assessment policies and governance structures, indicating required approvals, assessment frequency, and follow-up actions for control weaknesses or heightened residual risks.
- **Third-party Arrangements**: When engaging external consultants, LFIs should ensure services are delivered under stringent oversight by key personnel and avoid overreliance on consultants.

Assessing Inherent Risk (1/2)

Effective risk management is predicated on a **sound understanding of the risks** inherent to an entity's business model. While there are different methods to conduct a risk assessment, LFIs are generally expected to evaluate differing levels of risk associated with their customers, products and services, delivery channels, geographic locations and markets, and operating structure.

- The LFI should **utilize a standardized approach** to assessing its customers, products and services, and geographies..
- The risk assessment should **consider more granular risk factors** for each category of inherent risk.
- The LFI should **assign each factor a score or weighting** that reflects the level of risk associated with that risk factor.
- LFIs should ensure that the assessment of risk factors **includes quantitative data**.
- LFI should consider **enhancing their risk assessment with data provided by CBUAE**.
- The risk assessment should **consider high-risk factors**.

Assessing Inherent Risk (2/2)

LFIs are generally expected to evaluate, at a minimum, the differing levels of risk associated with their customers, products and services, delivery channels, geographic locations and markets.

Risk Factor	Description
Customers	An LFI's customer risk is based on the **characteristics** of its customer base, including the **concentration** of customers in risk-rated segments, customers' industries, professions, and entity type, and risk ratings of beneficial owners and other related parties, among other factors.
Products and Services	Product and service risk derived from the range of products and services that the LFI offers its customers, and whether those products and services have **characteristics** that present elevated ML/TF/PF risks.
Delivery Channels	Delivery channel risk stems from the extent to which an LFI's methods of account origination/customer onboarding, account servicing, and transaction facilitation, limits the LFI's understanding of its customers' identities, activities, and counterparties.
Geographies	Geographic risk stems from the LFI's exposure - through operating in certain (e.g. high-risk) locations (including those of any global affiliates and branches located outside of the UAE), having a customer base and/or transacting in regions and jurisdictions that present an elevated degree of ML/TF/PF risks.

Measuring Inherent Risk (1/2)

An LFI may choose to assess its inherent risk based on the **likelihood** that a ML/TF/PF risk event occurs and the **impact** should the ML/TF/PF risk event materialize.

- **Likelihood** = the potential for ML/TF/PF occurring.
- **Impact** = the damage that will be incurred if ML/TF/PF occurs.

Likelihood ✖ **Impact**

=

Inherent Risk

Likelihood scores rating

- **Very High**: Almost certain that a ML/TF/PF risk event will occur several times a year.
- **High**: High chance that a ML/TF/PF risk event will probably occur several times a year.
- **Moderate**: Moderate chance that a ML/TF/PF risk event will occur once a year.
- **Low**: Low chance but not impossible that a ML/TF/PF risk event will occur.
- **Incidental or Very Low**: Relatively no chance that a ML/TF/PF risk event will occur.

Impact assessment

- Assessed based on the possible regulatory, legal, financial, and reputational effects that could result if a ML/TF/PF event occurs. A five-level scale is provided as an example:
- **Catastrophic**: The most severe damage (such as resulting in the loss of a license).
- **Major**: Significant damage.
- **Moderate**: Moderate level of damage.
- **Minor**: Minimal level of damage.
- **Incidental**: Little or no damage.

Measuring Inherent Risk (2/2)

Below is an illustrative matrix for plotting likelihood and impact of a risk scenario to arrive at an LFI's inherent risk rating

Likelihood	Impact: Incidental - 1	Low - 2	Moderate - 3	Major - 4	Catastropic - 5
Very High - 5	Moderate - 5	High - 10	High - 15	Very High - 20	Very High - 25
High - 4	Moderate - 4	Moderate - 8	High - 12	High - 16	Very High - 20
Moderate - 3	Low - 3	Moderate - 6	Moderate - 9	High - 12	High - 15
Low - 2	Very Low - 2	Low - 4	Moderate - 6	Moderate - 8	High - 10
Very Low - 1	Very Low - 1	Very Low - 2	Low - 3	Moderate - 4	Moderate - 5

Risk Score

Assessing the Control Effectiveness (1/2)

Once inherent risks have been identified and assessed, LFIs should assess mitigating controls to determine how effectively they manage the institution's risks.

Best practices to assess the control environment:

- LFIs should map controls to specific drivers of inherent ML/TF/PF risk to ensure adequate coverage of mitigating controls.
- Each control area assessed should be assigned a score that reflects the relative strength of that control as well as a weighting based on the importance that the institution places on that control.
- The LFI should raise an action to remedy any identified deficiency if an action is not already underway.
- Control effectiveness assessments should be based on objective and quantifiable information tied to the controls.

Assessing the Control Effectiveness (2/2)

Mitigating controls include the LFI's policies, procedures, processes, systems, and effective implementation of risk-mitigating measures, which include overall governance and management oversight, CDD/KYC, internal controls, training, and independent testing or independent audit.

Control Factor	Description
Governance	An LFI's organizational structure and governance are key components to understanding and implementing AML/CFT/CPF controls and building an institution-wide culture of compliance.
CDD/KYC	A robust CDD/KYC program establishes the LFI's understanding of risks associated with each customer as well as each customer's expected activity, better enabling the institution to detect unusual or potentially suspicious transactions.
Internal Controls	Mitigating measures related to internal controls entail policies, procedures, and processes designed to limit and control risks associated with core operational elements of the LFI's AML/CFT/CPF program and achieve compliance with relevant laws and regulations.
Training	Training should be provided on an ongoing basis and include changes to regulations, internal policies or procedures, and an understanding of evolving AML/CFT/CPF risks to which the LFI is exposed.
Independent Audit	Independent Testing includes reviewing the LFI's policies, procedures, systems, and controls that mitigate and manage an LFI's ML/TF/PF risks and identifying any areas of the compliance program that may require remediation or improvement.

Quantifying Control Effectiveness

To quantify control effectiveness, an LFI should consider applying the following steps:

Identify Key Controls: LFIs should list all relevant controls that have been implemented to mitigate identified risks.

Define Effectiveness Criteria: LFIs should establish criteria to measure the effectiveness of each control.

Measure Performance Against Criteria: LFIs should collect data on how each control performs against the established criteria.

Scoring System for Controls: LFIs should develop a scoring system to rate the effectiveness of each control based on its performance.

Aggregate Control Scores: LFIs should calculate an overall control effectiveness score by aggregating the scores of individual controls.

Adjust for Interdependencies: LFIs should recognize and consider that controls might be interdependent.

Regular Updates and Reviews: Control effectiveness should be an ongoing concern, with regular updates and reviews, to ensure that controls are adapting to evolving risks.

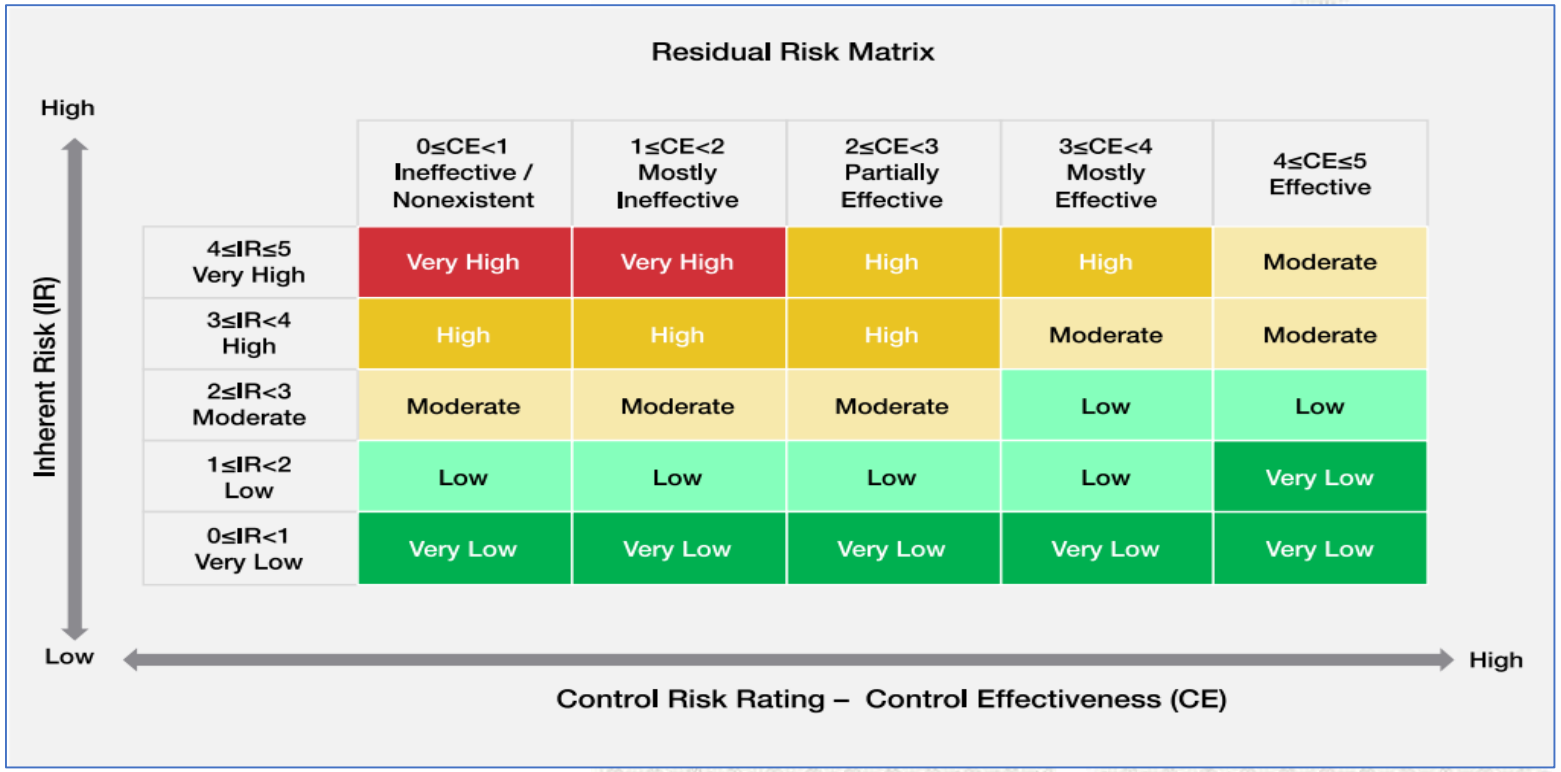
Documentation and Reporting: LFIs should keep detailed records of the evaluation process.

Determining Residual Risk

- Once both the inherent risk and the design and effectiveness of an entity's mitigating controls have been considered, risk assessments should determine the entity's overall residual risk.
- Overall enterprise-wide residual risk is a function of the total inherent risk to which the LFI is exposed to - through the customers, geographies, products, services, delivery channels, transactions, and operational factors; and the extent to which its controls effectiveness limits the real risk that the inherent risk exposure.
- Determining residual risk is important to identify the nature and extent of ML/TF/PF risks, so that the LFI's AML/CFT/CPF program can develop and implement tailored and effective risk mitigating measures, including dedicating additional human, technological, and financial resources to the areas of the entity's high risks.

Residual Risk Matrix

A common practice for determining overall residual risk is the utilization of a residual risk matrix that aligns inherent risk and mitigating controls ratings or scores to generate a residual risk rating or score, along a standardized assessment scale. Below is a sample residual risk matrix that utilizes a five-level scale for assessing inherent risks, mitigating controls, and the resulting residual risks.



Application of the Risk-Based Approach

Applying the Risk-Based Approach (1/2)

Once the LFI has identified and assessed the ML/TF/PF risks it faces, an LFI's Board of Directors, owners/partners/shareholders, or senior management should **revisit the LFI's risk appetite statement** to ensure it adequately reflects an institution's ML/TF/PF risk. The LFI's leadership should also assess whether they would like to lower the LFI's residual risk exposure by developing or updating AML/CFT/CPF controls and/or reducing exposure to inherent risks that cannot be managed effectively.

Based on this understanding, the LFI should **develop a detailed action plan** for the Board of Directors or owners/partners/shareholders that outlines new or updated AML/CFT/CPF controls for addressing inherent risks identified in the ML/TF/PF risk assessment, and include an estimated timeline of implementation. This action plan should take into account the RBA, such that if an LFI's residual risk increases, for instance, revealing that the LFI faces higher ML/TF/PF risks, the LFI may seek to develop enhanced measures to mitigate such higher risk by expanding the range, degree, frequency, and intensity of its AML/CFT/CPF controls.

Applying the Risk-Based Approach (2/2)

In accordance with an RBA, LFIs should mitigate identified risks through the implementation and updating of controls and measures tailored to these risks, such as:

- **CDD/KYC processes**, including customer and beneficial ownership identification and verification.
- **EDD measures:** in higher-risk scenarios obtain additional information on the customer and ensure enhanced ongoing monitoring and oversight of the customer relationship.
- **Ongoing CDD monitoring:** maintain current, accurate, and complete customer information and identify changes to the customer risk profile.
- **Transaction monitoring controls and measures** that detect and alert the LFI when customers have suspicious or unusual transactions.
- **Sanctions screening controls and measures** for screening customers and transactions against relevant lists.
- **Suspicious activity monitoring systems and processes** that are aligned to the institution's ML/TF/PF risk assessment.
- **Appropriate governance arrangements** under which responsibility for AML/CFT/CPF is clearly allocated.
- **Processes to recruit and vet staff** in line with the institution's level and type of ML/TF/PF risk.
- **Ongoing and role-based training** for AML/CFT/CPF staff on the institution's business activities.
- **Controls** to test the overall effectiveness of the institution's AML/CFT/CPF policies, procedures, and processes.

Next steps: Gap Analysis & Implementation

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Gap Analysis

- Licensed financial institutions (LFIs) are required to conduct gap analysis as part of their regulatory compliance obligations to ensure their internal policies, procedures, and systems align with current laws, regulations, and standards set by the Central Bank of the UAE (CBUAE).
- Gap analysis helps LFIs identify discrepancies between their current practices and the regulatory requirements, and allow them to address any shortcomings and strengthen their AML/CFT/CPF framework.

Implementation

- LFIs are expected to demonstrate they have taken concrete efforts to come into compliance with the Best Practice requirements within one month from its coming into effect

- Minimum expectation (additional to existing provisions) :

1) development of policies, procedures, and training materials, and
2) conduct of role-based training.

Conclusion and Questions

Thank You

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Thank You

CentralBankUAE
CentralBankUAE
Central Bank of the UAE

CentralBankoftheUAE
Central Bank of the UAE

المصرف-المركزي.امارات
www.centralbank.ae

Central Bank of the UAE:

Download on the App Store
GET IT ON Google Play

المصرف-المركزي.امارات
www.centralbank.ae