OUTREACH EVENT
on the
AML/CFT Guidance for Licensed Exchange Houses
and
Amended Chapter 16 of the *Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business*

12 January 2022

Outline of this Presentation

- Introduction
- The Risk Assessment
- The Compliance Officer
- Know Your Customer
  - CID, CDD, EDD
  - Special KYC Situations
- Wire Transfers
- Transaction Monitoring
- Sanctions Screening
- Reporting to the FIU
- Training
- Record Retention
- Internal Audit
- Q & A

Purpose & Applicability of the Guidance and amended Chapter 16 of the Standards

Purpose

- The Guidance does NOT constitute new regulation and does NOT introduce new legal obligations. It is designed to help CBUAE's LEH understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.
- In connection to the issuance of the Guidance, selected provisions of the Chapter 16 of the Standards for Licensed Exchange Houses (LEH) were updated to be aligned with the latest UAE AML/CFT law as well as other AML/CFT Guidances issued by the Central Bank in 2021.
- The Guidance and Standards came into effect on 17 November 2021, with LEH expected to demonstrate compliance with their requirements within one month from their coming into effect.

Applicability

The Standards and Guidance apply to all Licensed Exchange Houses that are licensed and supervised by the CBUAE.

Guidance: Exchange Business Risks

The Guidance acknowledges that most transactions carried out by LEH are legitimate. But there are still risks in the sector arising from:

The products and services LEH offer. LEH move funds across borders at high speeds.

Exposure to cash. LEH frequently receive cash and thus may unwittingly assist illicit actors to place the proceeds of crime in the financial system.

Customer relationships. LEH often do not establish full customer relationships but instead deal with customers on a transactional or a one-off basis.

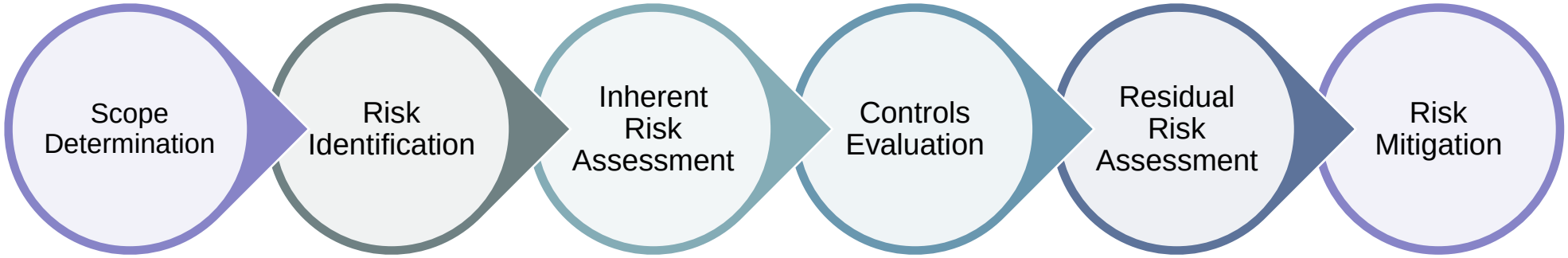
Global regulatory disparities. LEH are exposed to exchange houses in other countries which may be less well-regulated.

The Risk Assessment

Guidance: The Risk Assessment Process

LEH must **identify, assess and understand** the ML/FT risks associated with their businesses and perform an enterprise wide ML/FT risk assessment on a regular basis. It must develop a risk assessment in order to understand how and to what extent it is vulnerable to ML/FT, and help determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk.

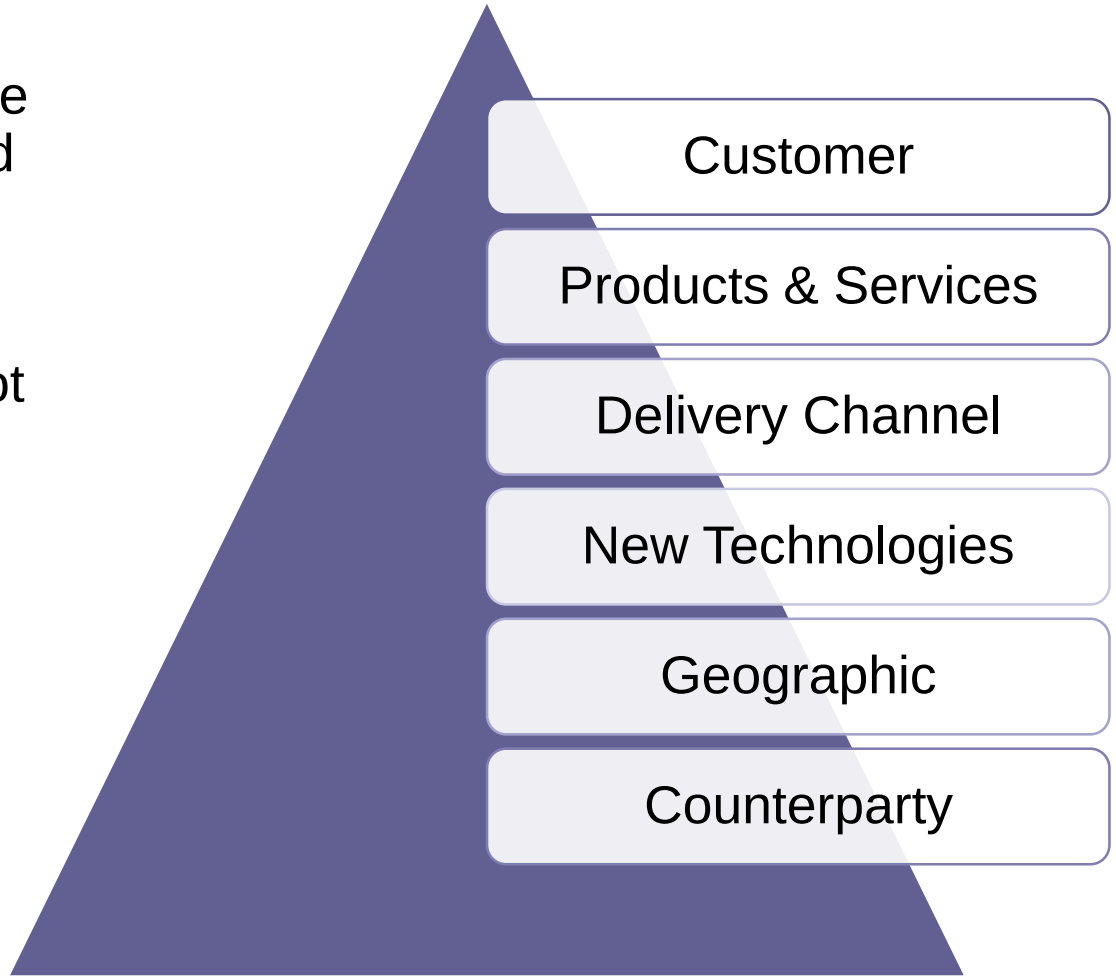
The risk assessment creates the basis for the LEH's risk-based approach. In general, the risk assessment process would entail the following six (6) steps:



For more information, please refer to the section on institutional risk assessment of the CBUAE's *AML/CFT Guidelines* as well as the associated outreach presentation published on CBUAE's website.

The nature and extent of any assessment of ML/FT risks must be appropriate to the nature, size, and complexity of the LEH's business.

The risk assessment should cover all relevant factors including but not limited to:



It must be regularly updated, annually at a minimum, as well as in response to major changes in the LEH's operations.

Risk Assessment and Risk Appetite

- In assessing ML/FT risks, the LEH must have the following elements in place:
  - Documented risk assessment methodology, procedures and processes.
  - Documented risk assessment findings, including determination of overall risk and specific risks, and mitigating measures to be applied to minimize the impact of risks.
  - Written risk appetite statement that clearly identifies the acceptable level of risk.
  - Appropriate mechanisms to provide information on risk assessments to the CBUAE when required.
- The risk appetite statement is a new requirement. An effective risk appetite statement will:
  - Clearly document the LEH's risk tolerance;
  - Specify products, services, and customer/transaction types that the LEH prohibits;
  - With the risk assessment, form the foundation for the AML program.

Updates to the Standards in this Area

Paragraph 16.2 of the Standards deals with the ML/FT risk assessment. This paragraph appeared in the previous version of the Standards, but the amended version includes important updates:

- Paragraph 16.2.1 requires that LEH must not only understand the ML/FT risks of their business but also perform an "enterprise wide ML/FT risk assessment" on a regular basis.
- Paragraph 16.2.3 lists the areas of risk that must be covered: New Technologies Risk is a new addition here.
- Paragraph 16.2.5(c) requires LEH to have a documented 'risk appetite statement' that "clearly identifies the acceptable level of risk."

The Compliance Officer

Guidance: Governance and the Compliance Officer

Every LEH must appoint a Compliance Officer and an Alternate Compliance Officer who are responsible for its AML/CFT Program. In order for these officers to be effective, it's critical that they, in particular:

- Understand risks in the sector and the risks the LEH faces;
- Have the necessary experience and expertise to do their jobs;
- Have sufficient staff/support and resources (including technology resources);
- Have clear authority over all aspects of the program;
- Have appropriate stature within the company, including the ability to raise issues directly to the Board or Owners/Partners as appropriate, without requiring permission from the Manager in Charge.

Updates to the Standards in this Area

Paragraphs 16.4-16.6 of the Standards covers requirements related to the Compliance Officer, the Alternate Compliance Officer and the Continuous Professional Development Programs (CPD). These paragraphs appeared in the previous version of the Standards and have been updated as follows:

- The Compliance Officer's duties must be strictly limited to AML/CFT compliance. For holders of Category B and C licenses, the Alternate Compliance Officer's responsibilities must also be limited to AML/CFT duties.
- The Compliance Officer must oversee the risk assessment and ensure that the LEH's transaction monitoring systems are appropriate and functioning as designed.
- The procedures related to notifying the BSD of new appointments and vacancies have been updated (emails and timelines). In particular, LEH must propose a replacement compliance officer to BSD within 90 days of the position falling vacant.
- All AML/CFT compliance staff must complete 48 hours of training within every 12-month period (previously upon the completion of a calendar year).

Know Your Customer

Guidance: Risk-Based KYC

1

The purpose of the KYC process is to ensure that LEH understand who their customer is and the purpose for which the customer will use the LEH's services**.** LEH must have a risk-based understanding of the customer and the risk that the customer and the customer's business could pose to the LEH.

2

KYC is not a check-the-box activity. The mandatory procedures are a minimum. An LEH can comply with all these minimum requirements and still be in violation if it carries out a transaction without taking a fully risk-based approach to understanding the customer and the related risks.

3

Risk-based KYC means that LEH apply additional efforts to understanding the customer or transaction where risks are higher due to the nature of the transaction, the products or services used, the delivery channel, the transaction or customer's geographic links, or what's already known about the customer.

Guidance: Ongoing Monitoring

- LEH must ensure that the documents, data and information obtained under CDD measures, which reflect their understanding of their customer, are up-to-date and accurate.
    - Customer risks may change regularly as individual customers change their activities/residence and as legal person customers may change their business, management, and ownership.
    - Ongoing monitoring allows LEH to ensure that the Exchange Business is being used in accordance with the customer or relationship profile developed through KYC during onboarding, and that transactions are normal, reasonable, and legitimate.
- The Standards include explicit requirements for when KYC must be updated and what information must be obtained.
- LEH should also consider a KYC update on a risk-based schedule and, for example, review the customer profile when the customer's behavior changes, when the customer's transactions/behavior have resulted in the filing of an STR/SAR with the FIU, when they have any concerns about the information on file, if they encounter any negative news about a customer, and whenever they feel it is necessary.

Updates to the Standards in this Area

Paragraphs 16.7 and 16.16 of the Standards outline the Know Your Customer ("KYC") process and identify the situations in which each type of KYC must be employed. Updates to these paragraphs include:

- The requirement that LEH understand the nature and intended purpose of the business relationship, as well as the nature of the customer's business and ownership and control structure.
- The requirement that LEH must not onboard the customer, must immediately terminate any relationship with the customer, must not execute any transaction, and should consider filing a STR, SAR or other reports with the FIU if they cannot carry out or complete CID/CDD/EDD as required.
- Transaction thresholds for when CID, CDD and EDD are required have also been updated (cf. slide 19).
- LEH must be able to demonstrate to the CBUAE that their KYC process is appropriate to their risks.
- Requirement of CID/CDD/EDD, as appropriate, must be conducted in person before a customer can use an ATM/Kiosk.
- Clarifications related to EDD requirements (cf. Slide 20).

When to Use Each KYC Type

Customer Type	Activity Type	Value of Transaction (AED)	Required KYC
Natural Persons	Currency Exchange	3,500 ≤ Value < 35,000	CID
		35,000 ≤ Value within a 90-day period < 55,000	CID **and** CDD
		55,000 ≤ Value within a 90-day period	CID, CDD **and** EDD
Natural Persons	Money Transfer	Value < 55,000	CID **and** CDD
		55,000 ≤ Value within a 45-day period	CID, CDD **and** EDD
Legal Persons & Arrangements	Any Activity	Any Value	CDD **and** EDD
Counterparties	Any Activity	Any Value	CDD **and** EDD
PEPs	Any Activity	Any Value	CID, CDD **and** EDD
DNFBP/DPMS	Any Activity	Any Value	CID (if natural person), CDD **and** EDD
High-Risk Natural Persons	Any Activity	Any Value	CID (if natural person), CDD **and** EDD
High-Risk Circumstances	Any Activity	Any Value	CID (if natural person), CDD **and** EDD
Third-Party Transactions	Any Activity	Any Value	CID(if natural person), CDD **and** EDD

Special Focus: When to Use EDD

LEH must not restrict EDD only to specific customer types for which it is directly required, but must use EDD whenever higher risks are present. In addition to the circumstances discussed in this presentation, LEH must use EDD when dealing with:

- Customers from high-risk jurisdictions;
- Unusually complex transactions or those with no clear legal or economic purpose;
- When suspicions of ML/TF are present;
- When there are any doubts about the veracity or adequacy of the information previously provided by a customer;
- When there is a material change in the nature or ownership of a legal person or arrangement customer (as part of required EDD for these customer types);
- And any other circumstance or customer type that an LEH views as higher-risk or where an LEH believes that EDD is required.

CDD and EDD for Natural Persons

Updates to the Standards in this Area

Paragraph 16.9 of the Standards covers **CDD requirements** for natural persons. Updates to paragraph 16.9 include:

- When verifying the Emirates ID card either physically, by way of digital or e-KYC solutions, LEH must use the online validation gateway of the Federal Authority for Identity & Citizenship, the UAE-Pass Application or other UAE Government supported solutions, and keep a copy of the Emirates ID and its digital verification record.
- The customer must be subject to PEP checks.
- Clarification of the requirements for ongoing monitoring and updating of the customer profile, which include:
  - Repeating CDD when the profile is reviewed or when there is a change in profile;
  - Reviewing the customer's past transactions to ensure that they are consistent with the customer's profile, source of funds, etc.;
  - Reviewing transaction monitoring results and STR filings to determine whether the customer's past behavior has generated alerts and STR/SAR.

Paragraph 16.10 covers **EDD requirements** for natural persons. Changes to this paragraph include, most importantly:

- A expanded definition of what EDD involves.
- Updated thresholds.
- An expanded discussion of the relationship between EDD and the existing requirement to give special attention to transactions by visitors in the UAE.

CDD and EDD for Legal Persons and Arrangements

Updates to the Standards in this Area

Paragraph 16.11 of the Standards covers CDD and EDD for legal persons and arrangements. LEH should carefully review the entire section, with some important changes consisting of:

- Extending coverage to legal arrangements as well as legal persons.
- Clarifying that LEH must perform both CDD and EDD for these customers.
- Updating the information collection requirements as part of CDD.
- Updating the requirements related to BO identification.
- Requiring LEH to assess and record the customer's expected annual activity as part of the CDD.
- As part of EDD, conduct a site visit to the customer's business location (where relevant) and assess the risk of the customer's customers.
- Requiring LEH to refresh CDD/EDD either annually or when a license/ID associated with the profile expires, whichever comes first, and introducing new requirements for ongoing monitoring.

LEH should carefully review the CBUAE's *Guidance for LFIs Providing Services to Legal Persons and Arrangements* and the associated outreach presentation.

Special Situations: FI Counterparts

Updates to the Standards in this Area

Paragraph 16.11.10 of the Standards has been updated with the requirements for CDD/EDD for foreign correspondent banking arrangements.

- As part of EDD for these relationships/customers, the LEH must collect sufficient information about any receiving correspondent institution for the purpose of identifying and achieving a full understanding of the nature of its business, and to determine, through publicly available information, its reputation and level of AML/CFT controls, including whether it has been subject to a ML/FT investigation or regulatory action.
- LEH must also evaluate the AML/CFT controls applied by the receiving correspondent institution and understand the responsibilities of each institution in the field of AML/CFT.

Special Situations: PEPs

Updates to the Standards in this Area

Paragraph 16.13 of the Standards covers Politically Exposed Persons (PEPs). Requirements related to PEPs are not new, but Paragraph 16.13 includes important updates:

- PEP requirements that previously applied only to FPEPs now apply to all PEPs. Heads of International Organizations are included in the definition of PEP.
- LEH must screen customer information to identify PEPs, and must re-screen customer profiles at least once a year.

Special Situations: DNFBPs & DPMS

Updates to the Standards in this Area

The amended Chapter 16 of the Standards introduces special EDD requirements for DNFBPs (16.14) and DPMS (16.15).

- Specific EDD is required for customers that qualify as DNBPs or DPMS, including those that are natural persons.
- LEH must have appropriate systems in place to identify customers who fit these definitions.
- LEH must ensure that these customers have the required licenses and are registered with the appropriate supervisor.
- They must also determine whether these customers comply with the AML/CFT requirements applying to them, and they must understand the customer's business and customer base.
- The Compliance Officer and Manager in Charge must approve the business relationships/transactions with these customer types.

LEH should carefully review the CBUAE's *Guidance for LFIs Providing Services to DPMS and the Real Estate Sector* and the associated outreach presentation.

Wire Transfers

Updates to the Standards in this Area

Paragraphs 16.17-19 of the Standards have been updated with the specific requirements when carrying out wire transfers.

It is important to note that under Cabinet Decision (10) of 2019, a wire transfer is very broadly defined as any “financial transaction conducted by a financial institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether or not the transferor and the beneficiary are the same person.” As a result, almost any money transfer carried out by an LEH is likely to be a wire transfer.

Paragraphs 16.17-19 detail the specific requirements for:

- Ordering institutions (those initiating a transfer on behalf of the customer sending money – Paragraph 16.17);
- Intermediary institutions (those facilitating a transfer between two other institutions – 16.18);
- Beneficiary institutions (those serving the customer receiving money – 16.19).

The primary goal of these requirements is to ensure that the originating institution includes information on the ordering and beneficiary customer with the transfer, and that this information is available to all financial institutions involved in the transfer chain.

Transaction Monitoring

Guidance: Transaction Monitoring

LEH must continuously monitor all their transactions to ensure they are consistent with the information the LEH has about the customer, the customer's activity, and customer risks.

Transaction monitoring systems allow the LEH to monitor the transactions made by their customers in real-time and/or on a daily basis to detect and investigate transactions that may need to be reported to the FIU because they are potentially related to illicit activity. Such a system is a required element of the AML/CFT program.

Transaction monitoring must be risk-based. This means that:

- The complexity and sophistication of your monitoring system must be consistent with the complexity and sophistication of your business;
- You must use monitoring rules and parameters that take into account your specific risks and ML/FT typologies in the Exchange House sector; and
- You must conduct more intensive monitoring of transaction types, customers, products/services, and delivery channels that you have identified as higher risk.

For more information, please refer to the *CBUAE Guidance for Licensed Financial Institutions on Transaction Monitoring Screening and Sanctions Screening* and the associated outreach presentation.

Updates to the Standards in this Area

Paragraph 16.24 of the Standards covers transaction monitoring and includes the following updates:

- Transaction monitoring rules must be risk-based, and must take account of ML/FT typologies in the Exchange Business sector.
- Reports made to the FIU must be considered as part of ongoing monitoring (as discussed above).

Sanctions Screening

Guidance: Sanctions Screening

LEH must conduct real-time sanctions screening to ensure that they comply with the requirement to immediately freeze all funds of a sanctioned person, and to observe the prohibition on providing funds or financial services to a sanctioned person.

LEH must sign up for the IEC's notification system to be notified of new designations.

LEH must sign up for the IEMS to ensure they are notified of requests for information, decisions of public prosecutions, and any other type of ML/FT-related request.

For more information, please refer to:

- the Executive Office of the IEC *Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions*;
- the *CBUAE Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*"; as well as
- the *CBUAE Guidance for Licensed Financial institutions on Transaction Monitoring and Sanction Screening;* and
- The associated outreach presentations.

Updates to the Standards in this Area

Paragraph 16.25 of the Standards discusses implementation of targeted financial sanctions, including screening obligations. There are very important updates in this paragraph and other paragraphs of the Standards that intersect with sanctions implementation, including:

- LEH must screen against the UAE's Local Terrorist List in addition to the UN List, and must register with the Executive Office of the IEC to receive updates to sanctions lists.
- LEH must use all information collected during the KYC process in screening.
- LEH must have procedures in place to test and fine-tune their screening software.
- Clarification that freezing requirement is "without delay and without prior notice," and extends to a prohibition on providing funds or any financial or related services to a sanctioned person.
- Clarification related to the reporting of screening outcomes (e.g. hits, funds frozen, etc.) via the goAML portal.

Reporting to the FIU

Guidance: STR/SAR Reporting

LEH must file without any delay a report with the UAE FIU, using the "goAML" portal, when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds in whole or in part, regardless of the amount, constitute the proceeds of crime, are related to crime, or are intended to be used in a crime.

- "*Reasonable Grounds*" – This does not mean indisputable evidence.
- "*Suspect*" – you need not be certain, and you should not wait until you are certain.
- "*Attempted transaction*" – you must file even if you turn a customer away or don't complete the transaction.
- "*In whole or in part*" – you don't need to suspect that all the funds in a transaction are related to a crime.

For more information, please refer to the *CBUAE Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting* and the associated outreach presentation.

Updates to the Standards in this Area

Paragraph 16.26 covers suspicious transaction reporting. The amended Chapter 16 of the Standards include important updates:

- Clarification that LEH must file reports to the FIU using the goAML portal when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds, in whole or in part, regardless of the amount, constitute the proceeds of crime, are related to a crime, or are intended to be used in a crime.
- Reports made to the FIU must be considered as part of ongoing monitoring (as discussed above).

Training

Guidance: Training

Training is critical to an effective AML/CFT program.

If employees don't understand their responsibilities, they are unlikely to be able to carry them out.

Employees should understand not only the processes they are required to follow, but also the risks these processes are designed to mitigate, and the possible consequences of those risks.

Employees should receive training that is tailored to the risks of the LEH and to their specific roles and responsibilities.

Comprehensive AML/CFT compliance training to all employees including its Manager in Charge, functional heads, Directors of the Board and Owner/Partners/Shareholders.

AML/CFT compliance training must be provided to all new joiners within thirty (30) calendar days from the date of joining.

All AML/CFT compliance staff must complete 48 hours of training within every 12-month period (CPD).

Non-compliance staff with higher-risk or more responsible roles should receive specialized training.

Training should be responsive to identified program concerns or deficiencies as well as regulatory changes and other relevant news.

Updates to the Standards in this Area

Paragraph 16.23 of the Standards covers the AML/CFT training program with clarification that the listed training topics should be covered in greater depth and additional topics selected on a risk-sensitive basis.

As discussed in the Compliance Officer Paragraph, special training requirements apply for compliance staff.

Record Retention

Updates to the Standards in this Area

Paragraph 16.29 of the Standards details the scope of requirements related to record retention with clarification that LEH must retain the following documents for **five years from the date of completion of the transaction, termination of the business relationship, or from the closing of the account**:

- Records, documents, data and statistics related to transactions;
- KYC and ongoing monitoring records;
- Copies of personal ID documents;
- Business correspondence;
- Training records;
- Results of STR/SAR filing analysis and STRs/SARs themselves (for 5 years from filing unless other circumstances require additional retention).

Independent Audit

Guidance: Independent Audit

- The purpose of the mandatory independent audit is to test the effectiveness and adequacy of the AML/CFT program and identify areas of weakness or where policies/procedures are not consistently followed.
- To effectively fulfil this purpose, independent audits, whether internal or external, must be comprehensive and should be carried out by qualified staff.
- To be effective, an audit should be the beginning rather than the end of a process.
  - Audit findings must be raised to the Board or the Owner/Partners.
  - The LEH must seek to quickly remediate negative findings and take steps to ensure that they don’t happen again.

Updates to the Standards in this Area

Paragraph 16.31 of the Standards covers independent audit. Although updates to this paragraph are brief, they are important:

- The external auditors must annually review implementation of all aspects of the AML/CFT laws and regulations, in particular Chapter 16 of the Standards.
- The Board must have in place procedures reasonably designed to ensure timely remediation of findings.

Questions