



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



UNITED ARAB EMIRATES
MINISTRY OF ECONOMY



الإمارات العربية المتحدة
وزارة الاقتصاد

UNITED ARAB EMIRATES
MINISTRY OF JUSTICE



الإمارات العربية المتحدة
وزارة العدل



ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

هيئة الأوراق المالية والسلع
SECURITIES & COMMODITIES AUTHORITY



ANTI-MONEY LAUNDERING & COUNTERING TERRORIST FINANCING GUIDELINES

إصدار

2021

Contents

1	Executive Summary	02	
	Purpose & Scope	04	
2	Summary of 2020-2021 Financial Institutions- Examination Practice	05	
	Governance Framework & Management Oversight	06	Monitoring & Surveillance 14
1.	ML/FT Risk Assessment	06	1. Transaction Monitoring Systems 14
2.	Three Lines of Defence	07	2. Sanctions Screening Systems & Processes 15
3.	Policies & Procedures	08	3. Suspicious Transaction Reporting 16
4.	AML/CFT Training Programme	09	
5.	Compliance Officer ("CO")/MLRO	10	Record Keeping Practices 17
	On-boarding and Continuous Monitoring of Customers	11	3 Summary of 2020-2021 DNFBPs- Examination Practices 18
1.	Customer Risk Rating Methodology	11	
2.	Customer On-Boarding Process & Customer Data Quality	12	Compliance Culture & Awareness 19
3.	Customer Due Diligence	13	ML/TF Risk Assessment 19
			Customer Due Diligence 20
			Policies & Procedures 21
			Internal Controls 22
			Suspicious Activity Reporting 22
			4 Conclusion 23
			5 Glossary 24

1-Executive Summary



In line with the UAE's National Strategy on Anti-Money Laundering and Countering the Financing of Terrorism, supervisors will continue to issue forward-looking guidance and will identify innovative practices that help improve the effectiveness of the UAE's AML/CFT supervision and its overall AML/CFT framework

H.E Khaled Mohamed Balama
Chairman of NAMLCFTC

Purpose & Scope

The content of this Joint Guidance is in line with the Financial Action Task Force (FATF) Recommendation 34 and Core Issue 3.6 stated in FATF's methodology guideline, which emphasises the importance of guidance, feedback and the need for supervisors to promote a clear understanding of regulatory obligations.

The Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organisations (otherwise known as the "AML Law"), and its implementing regulation, Cabinet Decision No. (10) Of 2019 concerning the Executive Regulation of Decree Law No. (20) Of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Illegal Organisations (otherwise known as the "AML/CFT Decision" or the "Cabinet Decision") were enacted to set out controls for the detection and prevention of Money Laundering and Terrorist Financing (ML/TF) activities, thereby safeguarding the integrity of the UAE's financial system.

Cabinet Decision No. (74) of 2020 regarding Terrorism Lists Regulation and Implementation of United Nation Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions was enacted to implement the United Nations and Local Targeted Financial Sanction regimes by all relevant entities in the UAE.

The Central Bank of the UAE (CBUAE), together with the Dubai Financial Services Authority (DFSA) of Dubai International Financial Centre (DIFC), the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM), the Securities and Commodities Authority (SCA),

the Ministries of Justice and of Economy (collectively the "Supervisory Authorities"), believe that specific contextual guidance to the sector is needed on AML/CFT standards. This Joint Guidance applies to all Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) (where applicable) licensed, registered and regulated by the Supervisory Authorities.

Common themes pertaining to "Satisfactory/Unsatisfactory" practices observed during inspections are outlined in the Joint Guidance.

Supervisory Authorities, applying a Risk-Based Approach (RBA) to supervision, have observed common themes during inspections from January 2020 to May 2021. Feedback to the sector on such learnings promotes the understanding of identifying, assessing and mitigating the risks of money laundering (ML), the financing of terrorism (FT), and the financing of illegal organisations, and assists them in performing their statutory obligations under the UAE's legal and regulatory framework. Each year, supervisory inspections would typically include only a number of supervised institutions in scope, targeting a percentage of the population. Therefore, feedback to the sector is imperative to enable supervisors to promote the application of risk-based AML/CFT and TFS obligations as broadly as possible, thereby reaching out to a larger number of FIs and DNFBPs.

The Supervisory Authorities in the United Arab Emirates (UAE) continue to monitor the evolving risk environment and remain agile in identifying emerging risks and responding promptly by issuing necessary guidance to the sector.

2-Summary of 2020-2021 Financial Institutions – Examination Findings

Inspections conducted on FIs during 2020-2021 focused on the review of the AML/CFT framework, the implementation of Targeted Financial Sanctions ("TFS") and Counter Proliferation Financing ("CPF").

From the inspections conducted, Supervisory Authorities have highlighted "Satisfactory/Unsatisfactory" practices that focus on key areas of assessment such as Governance Framework and Management Oversight, AML and Sanctions Compliance Risk Assessment Framework, Monitoring and Surveillance, and Record Keeping Practices.

Governance Framework & Management Oversight

1. ML/FT Risk Assessment

The AML/CFT Law and the AML/CFT Decision indicate that FIs **utilise a Risk Based Approach with respect to the identification and assessment of ML/FT risks**. FIs are obliged to assess and to understand the ML/FT risks to which they are exposed to, and how they may be affected by those risks.

The table below outlines examples of satisfactory and unsatisfactory practices in FIs' ML/FT Risk Assessments.



- Well-established concept of a RBA to identify and assess ML/FT, TFS and PF risks commensurate with the FI's risk profile, complexity and size.
- Comprehensive and clearly documented risk assessment and methodology that capture both qualitative and quantitative measures, including group operations.
- Dynamic risk assessment that is regularly updated as soon as emerging risks are identified.
- Responsibilities are clearly defined and documented across the organisation.
- The results from the risk assessment are clearly linked to the Risk Appetite Statement and other risk assessments/monitoring tools.
- The FI considers ML/FT, TFS and PF risks when developing new products and business practices, as well as new and developing technologies.



- Lack of quantitative analysis of the FI's customer base considering the four elements - customer, product and services, delivery channel and geography - to identify inherent risk.
- The risk assessment is not granular to understand specific products and services, or industry and business types of FIs.
- No consideration of the results from the National Risk Assessment (NRA).
- No coverage of FI's obligations relating to PF, fraud and tax.
- Results of internal control testing (e.g. Risk Control Self Assessment /Internal Audit/Compliance Monitoring) of the FI is not incorporated in the risk assessment, hence the determination of residual risk is inaccurate.

2. Three Lines of Defence

FIs must **implement an effective risk culture and internal controls** across the institution and its subsidiaries, affiliates and international branches. In setting up the Three Lines of Defence Model, FIs can take into account their business nature, size and complexity.

The table below outlines examples of satisfactory and unsatisfactory practices within the Three Lines of Defence Model.



- Front line staff are well equipped and have the right access to the systems to perform their duties by receiving adequate training tailored to their specific responsibility or function, and have sufficient knowledge and information to effectively implement FIs' AML/CFT policies and procedures.
- An Independent Compliance Monitoring programme is in place to identify ML/FT risks and monitor and test AML/CFT controls.
- Third and Second line staff have detailed AML/CFT work programmes in place to test control effectiveness.
- Feedback loops across all three lines of Defence are established to constantly improve control design and effectiveness.



- Front line staff fail to take the necessary ownership to identify ML/FT risks associated with the customer and are not well equipped to perform their duties.
- Front line staff have weak understanding and insufficient training on ML/FT risks associated with products and services.
- AML/CFT processes are not subject to regular independent reviews.

3. Policies & Procedures

FIs must **develop clear and simple steering documents** that are uniform across the entire organisation and **must incorporate comprehensive procedures**, which translate the AML/CFT policies into an acceptable and workable practice, tasking the stakeholders with their respective responsibilities.

The table below outlines examples of satisfactory and unsatisfactory practices in financial institutions' policies and procedures.



- FIs have comprehensive policies and procedures that are commensurate with the nature and size of the FI and are communicated to all staff.
- Policies and procedures are approved by the appropriate body in the organisation (e.g. Board, Senior Management) and are continuously reviewed for effectiveness and periodically updated. They apply to all branches, subsidiaries and affiliated entities within the group.
- FIs have implemented a clear process to update policies and procedures for new regulatory requirements. Documents are easily available to all concerned staff and major changes are communicated in a timely manner.



- Policies and procedures are not updated regularly and are not comprehensive to cover all areas of ML/FT and PF risks.
- Internal policies, controls and procedures do not reflect the results of the FI's ML/FT risk assessment.
- Changes in policies and procedures are not communicated in a timely manner. Concerned staff are unaware of changes and do not have access to the documents.

4. AML/CFT Training Programme

FIs must **develop a robust and comprehensive risk-based training programme** that mitigates ML/FT risks to which they may be exposed.

The table below outlines examples of satisfactory and unsatisfactory practices in the financial institutions' Training Programme.



- Specialised training is offered to staff operating in high-risk segments of the FI (e.g. Trade Based Money Laundering training offered to Trade Finance staff).
- Training needs are continuously identified and a training plan including the necessary budget is approved.
- The FI has defined a maximum timeframe to complete mandatory training for new joiners and follow ups must be conducted.
- Assessments post training are completed to evaluate staff knowledge and understanding.
- All staff (including Senior Management and the Board) are subjected to AML/CFT training on an ongoing, yearly basis at a minimum.



- Weak training programmes that do not comprehensively cover AML/CFT laws and regulations.
- Generic training is provided to all employees. No controls implemented to ensure that missed training is completed at a later date.
- New joiners do not receive mandatory training and no close monitoring and follow ups are conducted.
- Training does not include assessments - hence success/failure cannot be measured and staff understanding cannot be assessed.
- Training programmes do not comprehensively cover the FI's policies and procedures used to mitigate ML/FT risks.

5. Compliance Officer ("CO") /MLRO

FIs are obliged to **appoint a compliance officer (CO) with the appropriate competencies and experience** to perform the statutory duties and responsibilities associated with this role.

The table below outlines examples of satisfactory and unsatisfactory practices associated with a CO.



- The CO is independent and has sufficient seniority to influence management and access relevant information.
- The CO is knowledgeable, competent and is involved in training to all staff.
- The CO plays an active role in the identification and reporting of suspicious transactions.



- The CO is not given support by Senior Management to execute his/her daily responsibilities.
- The CO has limited involvement in developing the AML/CFT programme.
- The CO does not have sufficient resources and/or access to information in order to perform their duties effectively.

On-boarding and Continuous Monitoring of Customers

1. Customer Risk Rating Methodology

FIs must ensure customers are risk rated in accordance with the policy, and develop an automated model to apply a customer risk rating based on different risk factors according to the nature, complexity, size, products and services, delivery channels, business segments and jurisdictions.

The table below outlines examples of satisfactory and unsatisfactory practices in the articulation of the Customer Risk Rating Methodology.



- Clear documentation of customer risk assessment and risk-rating methodology and ensuring they remain up to date on an ongoing basis.
- Customer risk rating is automated and takes into account customer's KYC profiles and post-triggered events that are detected in the Transaction Monitoring System.
- Actual transactions and risk indicators are considered (i.e. high turnover, cash intensity, transactions with high-risk jurisdictions).
- Country risk categorisation is supported by a documented rationale and is in line with counter measures regarding High Risk Countries as per the Financial Action Task Force (FATF) high-risk and other monitored jurisdictions.



- The customer risk rating methodology does not include all risk factors (customer /product /geography/channel).
- Customer risk ratings are manually assigned for complex profiles.
- Risk rating can not be refreshed periodically because the data necessary to do so is not available in the system.
- Customer risk ratings are a 'one-off' exercise and are not subject to regular review.
- Front line staff are able to lower a risk rating without sufficient justification.

2. Customer On-Boarding Process & Customer Data Quality

The **quality and completeness of the KYC data is the fundamental building block** for the entire regulatory and compliance framework, including customer risk assessment, customer due diligence, sanctions screening and transaction monitoring.

FIs are prohibited from establishing or maintaining any customer or business relationship, conducting any financial or commercial transactions, keeping any accounts under an anonymous or fictitious name or by pseudonym or number.

The table below outlines examples of satisfactory and unsatisfactory practices in the Customer On-Boarding Process and Customer Data Quality.



- System validation controls are in place to ensure mandatory data is entered in the system and is subsequently kept current.
- Comprehensive and regular training is provided to staff to ensure data quality errors are identified and rectified.
- Data quality programmes are in place that address shortcomings identified on customer data.
- Known gaps in data quality are remediated on a high priority basis using adequate manpower and budget. Progress is monitored closely and communicated to all relevant stakeholders. Additional controls are put in place to monitor risks adequately.



- Inconsistent data stored in core systems.
- Concerned staff are not aware of data requirements during customer onboarding (i.e. data collection through onboarding, including KYC form and data entry in core banking/KYC system).
- Limited assurance checks in core systems and customer on-boarding processes.
- Data gaps are either not identified or not remediated in a timely manner due to unclear responsibilities and budget constraints.
- Failure to review and update information on a regular basis.

3. Customer Due Diligence

FIs are obliged to **undertake appropriate customer due diligence (CDD) measures** at the time of onboarding and ongoing due diligence throughout the business relationship.

The table below outlines examples of satisfactory and unsatisfactory practices within the Customer Due Diligence Process.



- Risk profile of customers should be commensurate with the types and levels of risk identified by the institution.
- Customer profiles are clearly documented for the intended purpose and nature of the business relationship.
- Ongoing due diligence is performed for customers/business relationships to ensure that the transactions conducted are consistent with the information maintained by the FI and the type of activity they are engaged in.
- Adequate controls are in place to ensure transactions are not undertaken before completing CDD verification.



- Inaccurate assessment of the customer/business relationship risk and incorrect risk classification of customers that leads to incorrect CDD measures applied.
- Customer information and account opening forms that are incomplete and/or invalid and contain expired KYC documents during file reviews.
- KYC reviews are limited to the update of expired identification documents. Changes in activity that are not commensurate with the customer's profile or business activity are not identified.
- Inadequate measures in place to identify ultimate beneficial owners or controllers.

Monitoring & Surveillance

1.Transaction Monitoring Systems

FIs **must have indicators in place to identify the suspicion of the occurrence of the crime in order to report Suspicious Transaction Reports (STRs). These indicators should be updated on an ongoing basis.** Such indicators support the detection of money laundering and terrorist financing activities. FIs must ensure the indicators are in line with their size, operations and risk profile.

The table below outlines examples of satisfactory and unsatisfactory practices in the Transaction Monitoring System (TMS).



- Typology assessments and documented rationale for scenarios implemented should be in line with the FI's size, risk profile and operations.
- TMS is comprehensive and monitors all transactions performed by the FI in all areas of business, ensuring risk-based business segments and thresholds are in place based on regular typology assessments and TMS tuning initiatives.
- The FI remains responsible for TMS and its parameters and is able to explain the approach taken to the regulator.
- Automated risk-scoring model for prioritizing alerts integrated within TMS.
- Specialized training conducted to responsible staff enabling them to detect the risks associated with the products and services, delivery channels, and customers when clearing alerts/cases in TMS.
- Grouping of transaction monitoring parameters and thresholds into risk scenarios, which in turn help FIs to more precisely target transaction patterns and behaviours in line with known ML/FT typologies.
- Sophisticated reporting mechanisms and dashboards such as TMS alert/case aging reports and alert/case analysis reports.



- Typology assessment, segmenting of business lines and threshold settings are not in line with the FI's nature, complexity of business, NRA and Risk Assessment.
- Once implemented, scenarios, business lines and thresholds are not validated to ensure that they remain relevant and current.
- Implementation and tuning of TMS is solely done by an external vendor without the FI's contribution and ability to understand and question the approach chosen by the external vendor.
- Detection scenarios are not calibrated to generate alerts for all AML/CFT and TFS typologies, products (i.e. trade finance) and payment channels (i.e. wire transfers, cash withdrawals, cheque deposit), and aggregated transactions.
- Transaction monitoring scenarios do not integrate PF components involving accounts of the individuals and entities deemed as higher risk for PF. This includes individuals associated with sanctioned activities, trading in strategic goods or commonly implicated in proliferation financing activities (i.e. shipping companies, exchanges houses, etc.)
- Weak analysis performed during alert/case investigations, where obvious red flags and underlying risks are not considered.
- Failure to identify dual use goods in transactions.

2. Sanctions Screening Systems & Processes

FIs must fulfil their obligations to **comply with the directives of the relevant Competent Authorities and Supervisory Authorities with regards to TFS and other decisions issued by the UN Security Council**. They must also manage their exposure to the risks associated with unilateral international financial sanctions programmes and restrictive measures implemented by other countries.

The table below outlines examples of satisfactory and unsatisfactory practices in Sanction Screening Processes.



- Clear methodology in the sanctions screening programme and maintenance of relevant and up-to-date controls in order to effectively implement TFS obligations.
- Investment in robust sanctions screening systems and periodically fine-tuning them.
- Specialised resources in the field of Sanctions.



- Weaknesses in the effectiveness of sanctions' screening systems and controls, thereby limiting the FI's ability to detect sanctioned individuals/entities.
- Inadequate processes and practices to sanction-screen individuals/entities as per their identification documents.
- Weaknesses in the fuzzy matching logic parameters at an on-boarding level, and weak documented logic for sanctions screening and threshold optimisation.

3. Suspicious Transaction Reporting

FIs are obliged to **report to the Financial Intelligence Unit (FIU) suspicious transactions** and any additional information required in relation to them, and also put in place and update **indicators that can be used to identify the suspicion of a crime involving ML/FT**.

The table below outlines examples of satisfactory and unsatisfactory practices in reporting STRs to the FIU.



- Maintenance of complete monitoring records, documents and information obtained in the course of analysing or investigating potentially suspicious transactions in the case management system.
- Clear internal processes to report STRs in a timely manner with an escalation/ reporting mechanism in place to Senior Management when timelines are breached.
- There is a clear process to ensure the reasons for filing a report to the FIU and any internal actions taken are recorded.



- Delays in the investigation undertaken, and/or investigations, are not supported by an adequate rationale.
- No clear timeframe or turnaround time (TAT) defined in standard operating procedures (SOPs) to report STRs to the FIU.
- The CO reports all internal referrals to the FIU without considering whether they are actually suspicious.

Record Keeping Practices

FIs are obliged to **maintain detailed records, documents, data and statistics for all transactions**, all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, as well as a variety of record types and documents associated with their ML/FT risk assessment and mitigation measures.

The table below outlines examples of satisfactory and unsatisfactory practices in Record Keeping Practices.



- Digital record keeping framework in line with record-keeping requirements, including retention and retrieval of records (both physical and electronic).
- Documents are linked to customer information number/file (CIN/CIF).
- Usage of optical character recognition (OCR) software to convert scanned copies into searchable data (i.e. Trade Finance).
- All records can be retrieved without delay, including where held by third parties or the parent company.



- Documents in the system that do not have a clear naming taxonomy.
- Inadequate process of storing records and delays in retrieving documents.
- Records are not kept or stored as per the AML/CFT Law and the AML/CFT Decision and/or cannot be retrieved easily.

3-Summary of 2020-2021 DNFBPs – Examination Findings

Inspections conducted on DNFBPs during 2020-2021 emphasised the need to review the AML/ CFT framework and the implementation of TFS and Counter Proliferation Financing (“CPF”).

From the inspections conducted, Supervisory Authorities have highlighted “Satisfactory/ Unsatisfactory” practices observed, particularly in the sectors outlined below:

1. Brokers and Real estate agents;
2. Dealers in precious metals and precious stones; and
3. Lawyers, notaries, and other independent legal professionals

A particular focus was on key areas of assessment such as Compliance Culture and Awareness, ML/FT Risk Assessment, Customer Due Diligence, Policies and Procedures, Internal Controls, and Suspicious Activity Reporting.

Compliance Culture and Awareness

Senior Management and the Board of Directors in the organisation are ultimately responsible for the **quality, strength and effectiveness** of the DNFBP's AML/CFT framework, as well as for the **robustness of its compliance culture**.

The table below outlines examples of satisfactory and unsatisfactory practices in the Compliance Culture.



- AML training programme is updated regularly and focuses on embedding a compliance culture and creating awareness.
- Front line staff have easy access to Senior Management to highlight day-to-day operational AML/CFT challenges.



- The infrastructure and processes are not commensurate with the institution's size, complexity of commercial transactions, cash dealings, products and services, delivery channels, and the jurisdictions within which it operates.
- Inadequate AML/CFT training programmes.

ML/FT Risk Assessment

DNFBPs must **identify, assess and understand the ML/FT risks** when preparing business-wide ML/FT risk assessments. The purpose of developing an ML/FT business risk assessment is to improve the effectiveness of ML/FT risk management, by identifying the inherent ML/FT risks faced by the enterprise as a whole and determining how these risks are **effectively mitigated through internal policies, procedures and controls**, and establishing the residual ML/FT risks and any gaps in the controls that should be addressed.

The table below outlines examples of satisfactory and unsatisfactory practices in ML/FT Risk Assessments.



- Assessing ML/FT risks associated with business lines and processes are considered.



- Weak understanding of its own risks, vulnerabilities and threats in light of its operations in high-risk industries and vulnerabilities to ML/FT.

Customer Due Diligence

The accurate assessment of customer/business relationship risk is fundamental to the risk classification of customers and the **effective application of appropriate risk-based customer due diligence measures**.

The table below outlines examples of satisfactory and unsatisfactory practices in Customer Due Diligence.



- Adequate risk classification is assigned, depending on the nature and size of the customer's business and of the risks involved.
- EDD files are approved by Senior Management.
- There are clear guidelines in undertaking customer due diligence measures, including customer acceptance and different risk factors of customers, considering counter measures regarding High Risk Countries as per the Financial Action Task Force ('FATF') high-risk and other monitored jurisdictions.
- Escalation metrics are in place to report to Senior Management in instances where KYC files are not in line with risk appetite.



- Incorrect assignment of the risk category as per the organisation's policy.
- Deficiencies in the identification of the customer's source of wealth.
- Deficiencies in the identification/ understanding of the ownership and control structure of a corporate entity.
- The same CDD measures are applied to all customers, irrespective of the risk rating.

Policies & Procedures

DNFBPs must **develop clear and steering documents** that are uniform across the entire organisation, and **must incorporate comprehensive procedures**, which translate the AML/CFT policies into an acceptable and workable practice, tasking the stakeholders with their respective responsibilities.

The table below outlines examples of satisfactory and unsatisfactory practices in DNFBPs' Policies and Procedures.



- Policies and procedures are approved by Senior Management and communicated to all employees of the institution.
- Policies and procedures are clear and stipulate the obligations of the AML/CFT Law and the AML/CFT Decision and are frequently updated with necessary amendments and improvements.
- Documented policies specific to high-risk customers and corresponding procedures, including escalation process to senior management.
- Well-documented processes that can help identify any unusual customer activity and to raise and report any suspicions.

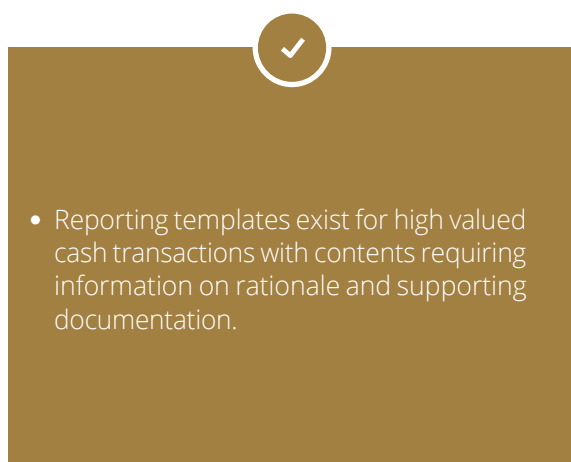


- Policies and procedures do not comprehensively cover all obligations stipulated in the AML/CFT Law and the AML/CFT Decision.
- Internal policies do not apply to branches, subsidiaries and affiliated entities.
- Failure to review policies and procedures following changes to legislation.

Internal Controls

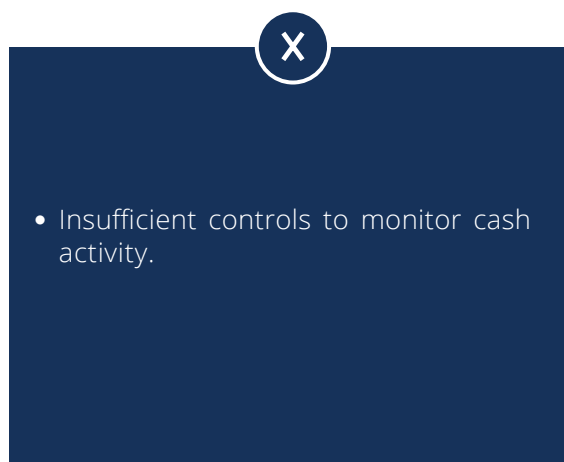
DNFBPs must **develop strong internal controls** that take into account whether the AML/CFT controls are effective, specifically whether they are adequate enough to mitigate risks concerning customers, products and services and/or transactions.

The table below outlines examples of satisfactory and unsatisfactory practices in Internal Controls.



A brown rectangular box with a white circle containing a checkmark at the top center. Inside the box, there is a single bullet point.

- Reporting templates exist for high valued cash transactions with contents requiring information on rationale and supporting documentation.



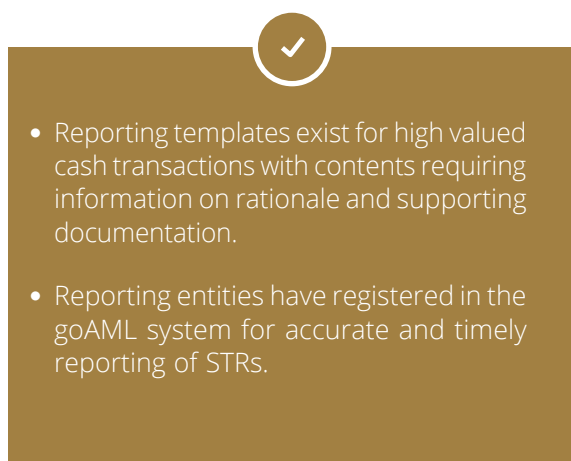
A dark blue rectangular box with a white circle containing an 'X' at the top center. Inside the box, there is a single bullet point.

- Insufficient controls to monitor cash activity.

Suspicious Activity Reporting

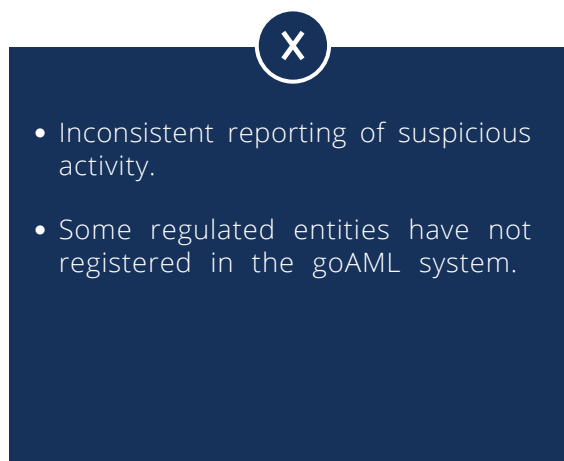
DNFBPs are obliged to **promptly report to the FIU on suspicious activities and any additional information related to them** when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime.

The table below outlines examples of satisfactory and unsatisfactory practices in Suspicious Activity Reporting.



A brown rectangular box with a white circle containing a checkmark at the top center. Inside the box, there are two bullet points.

- Reporting templates exist for high valued cash transactions with contents requiring information on rationale and supporting documentation.
- Reporting entities have registered in the goAML system for accurate and timely reporting of STRs.



A dark blue rectangular box with a white circle containing an 'X' at the top center. Inside the box, there are two bullet points.

- Inconsistent reporting of suspicious activity.
- Some regulated entities have not registered in the goAML system.

4-Conclusion

Supervisory Authorities remind FIs and DNFBPs to remain abreast of all regulatory obligations under the UAE Federal Decree Law on AML/CFT and Financing of Illegal Organisations, and its Implementing Regulation, Instructions, Guidelines, Notices, and Rules ('AML Legislation').

The mitigation of ML/FT crimes and effective control measures remain a key priority for the UAE.

If any further concerns arise or assistance is required, FIs and DNFBPs should contact their respective Supervisory Authority.

5-Glossary

- **AML/CFT** - Anti-Money Laundering and Countering the Financing of Terrorism.
- **Crime** - Money Laundering crime and related predicate offences, or Financing of Terrorism or Illegal Organisations.
- **CDD** - Process of identifying or verifying the information of a customer or beneficial owner, whether a natural or legal person or a legal arrangement, and the nature of the activity and the purpose of the business relationship and the ownership structure and control for the purposes of the Decree-Law and its affiliated Decision.
- **Competent Authorities** - The competent government authorities in the State entrusted with the implementation of any provision of the Decree-Law and the present Decision.
- **Customer** - Any person involved in or attempts to carry out any of the activities specified in the Implementing Regulations of the Decree-Law (Articles 2 and 3 of the Cabinet Resolution) with one of the Financial Institutions or Designated Non-Financial Businesses and Professions.
- **Decree-Law (or “AML-CFT Law”)** - Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations.
- **Decision (or “AML-CFT Decision” or “Cabinet Decision”)** - Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
- **Designated Non-Financial Businesses and Professions (DNFBPs)** - Anyone who conducts one or several of the commercial or professional activities defined in Article (3) of the Cabinet Decision, being anyone who is engaged in the following trade or business activities:
 1. Brokers and real estate agents when they conclude operations for the benefit of their customers with respect to the purchase and sale of real estate.
 2. Dealers in precious metals and precious stones in carrying out any single cash transaction or several transactions that appear to be interrelated or equal to more than AED 55,000.

3. Lawyers, notaries, and other independent legal professionals and independent accountants, when preparing, conducting or executing financial transactions for their customers in respect of the following activities:

- (a) Purchase and sale of real estate.
- (b) Management of funds owned by the customer.
- (c) Management of bank accounts, saving accounts or securities accounts.
- (d) Organising contributions for the establishment, operation or management of companies.
- (e) Creating, operating or managing legal persons or legal arrangements.
- (f) Selling and buying commercial entities.

4. Providers of corporate services and trusts upon performing or executing a transaction on behalf of their customers in respect of the following activities:

- (a) Acting as an agent in the creation or establishment of legal persons.
- (b) Working as or equipping another person to serve as Director or Secretary of a company, as a partner or in a similar position in a legal person.
- (c) Providing a registered office, work address, residence, correspondence address or administrative address of a legal person or legal arrangement.
- (d) Performing work or equipping another person to act as a trustee for a direct trust or to perform a similar function in favour of another form of legal arrangement.
- (e) Working or equipping another person to act as a nominal shareholder in favour of another person.

5. Other professions and activities that shall be determined by a decision of the Minister.

- **Financial Institution** - Anyone who conducts one or several of the financial activities or operations of/or on behalf of a Customer.
- **Financial Transactions or Activities** - Any activity or transaction defined in Article (2) of the Cabinet Decision.
- **Financing of Illegal Organizations** - Any physical or legal action aiming at providing funding to an illegal organization, or any of its activities or members.
- **Money Laundering (ML)** - Any of the acts mentioned in Clause (1) of Article (2) of the Decree-Law.
- **Proliferation financing (PF)** - Provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
- **Risk Based Approach** - A Risk Based Approach is a method for allocating resources to the management and mitigation of ML/FT risk in accordance with the nature and degree of the risk.
- **Supervised Institutions** - Financial Institutions (FIs), Designated Non-Financial Businesses and Professions (DNFBPs) which fall under the scope of Federal Decree-Law No. (20) Of 2018 on Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, and of Cabinet Decision No. (10) Of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
- **Supervisory Authority** - Federal and local authorities, which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions and Non-Profit Organisations or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislation.
- **Suspicious Transactions** - Transactions related to funds for which there are reasonable grounds to believe that they are earned from a misdemeanour's or felony or related to the Financing of Terrorism or of illegal Organisations, whether committed or attempted.
- **Targeted Financial Sanctions** - Targeted Financial Sanctions are part of an international sanctions regime issued by the UN Security Council under Chapter (7) of the United Nations Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.
- **Transaction** - Any business of either dealing, structuring, advising, drafting, appearing, arranging for funding or investing, preparing documentation or disposal or use of funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation.

