



Regulatory Update

Middle East, April 2026

Issued 12 May 2026



Table of Contents

1. DIFC AND DFSA LATEST DEVELOPMENTS.....	4
1.1 DFSA Signs MoU	4
1.2 DFSA Announces Temporary Regulatory Relief Measures	4
1.3 DIFC Introduces Temporary Economic Support Measures	4
1.4 DFSA Publishes Thematic Review Findings	5
1.5 DFSA Issues Liquidity Survey	5
1.6 DFSA Issues Survey on Marketing and Selling Foreign Funds	5
1.7 DFSA Issues Revisions to the Business Continuity Measures	6
1.8 DFSA Issues Two Alerts	6
1.9 DIFC Announces AI-Native Financial Centre	6
1.10 DFSA Issues Dear Finance Officer Letter on EPRS Reporting Errors	7
1.11 DFSA Publishes Summary of Consultation Paper 170	7
2. ADGM AND FSRA LATEST DEVELOPMENTS	8
2.1 ADGM RA Issues Warning	8
2.2 FSRA Issues Guidance on Business Risk Assessment	8
2.3 FSRA Issues Reminder on 2025 AML Return	8
2.4 FSRA Conducts Virtual Outreach Session on UAE FATF Mutual Evaluation	8
2.5 FSRA Publishes Dear SEO Letter	10
2.6 ADGM Amends Its Commercial Legislation	10
2.7 FSRA Implements Enhancements to Insurance Regulatory Framework	10
2.8 FSRA Publishes Updates to Staking Regime	11
2.9 FSRA Issues Two Regulatory Alerts	11
2.10 FSRA Issues Consultation Paper on AML Framework Enhancements	12
2.11 FSRA Issues Cyber Threat Notice for VASPs	12
3. MIDDLE EAST REGULATORY UPDATES	13
3.1 CMA Issues Request for Economic Impact Assessment	13
3.2 UAE Authorities Revise Administrative Tax Penalties	13
3.3 CMA Issues Dear CEO Letter on Key AML/CFT/CPF Obligations	13
3.4 CBUAE Launches Unified e-KYC Platform	15
3.5 CBUAE Updates AML/CFT/CPF Guidance	15
3.6 SSC Issues Guidance on CO/MLRO Function	15
3.7 CMA and FIU Hold Awareness Session on Reporting	16
3.8 CMA Issues VASP and ATS Regulations	17
3.9 CMA Launches Open Data Portal	18
3.10 CMA and UASA Deliver Professional Development Programmes	18
3.11 CMA Issues Several Warnings	18

4.	INTERNATIONAL UPDATES.....	19
4.1	UNSC Updates Sanctions List.....	19
4.2	FATF Holds Ministerial Meeting	19
4.3	World Alliance Releases 2026 Report on Artificial Intelligence in Financial Services	19
4.4	MENAFATF Chairs Joint Supervisory Authorities Forum	20
	ABOUT WAYSTONE COMPLIANCE SOLUTIONS	21

1. DIFC AND DFSA LATEST DEVELOPMENTS

1.1 DFSA Signs MoU

On 2 April, the Dubai Financial Services Authority ('DFSA') and the UAE Ministry of Economy and Tourism signed a Memorandum of Understanding ('MoU') aimed at strengthening regulatory cooperation, enhancing oversight of auditors and Designated Non-Financial Businesses and Professions ('DNFBPs'), and supporting the continued growth and integrity of the UAE's financial services sector.

You can read the DFSA announcement in full [here](#).

1.2 DFSA Announces Temporary Regulatory Relief Measures

On 9 April, the DFSA introduced a package of temporary and proportionate regulatory relief measures to support both newly applying firms and existing Regulated Entities within the Dubai International Financial Centre ('DIFC'). The measures were intended to provide operational flexibility during the exceptional operating environment, while ensuring firms continue to meet the DFSA's high regulatory standards.

Key areas of temporary relief include:

- authorisation and licensing flexibility
 - o adjusted timelines and administrative relief for firms seeking DFSA authorisation
 - o supervisory deadlines may be extended where appropriate to accommodate operational constraints
- governance and staffing adjustments
 - o flexibility around governance arrangements and key function holders, recognising remote-working dynamics and temporary changes in staff location
 - o relief is calibrated to ensure continued oversight without compromising independence or control functions
- regulatory reporting and supervisory processes
 - o extended reporting deadlines and modified supervisory expectations to allow firms to prioritise critical operations
 - o temporary easing of certain administrative requirements to reduce operational burden
- implementation timelines for regulatory initiatives
 - o postponement of selected regulatory projects where delays do not undermine regulatory outcomes
 - o intended to give firms additional capacity to manage internal and external challenges.

The DFSA reaffirmed its commitment to supporting the DIFC financial community during this period.

You can read the DFSA announcement in full [here](#).

1.3 DIFC Introduces Temporary Economic Support Measures

On 9 April, the DIFC announced a targeted package of temporary economic support measures designed to assist its business and retail community as the region transitions out of the recent operating environment. These measures took immediate effect and were intended to ease short-term operational and financial pressures on firms.

The DIFC Authority introduced a range of initiatives, including flexible payment arrangements for retail and commercial tenants, instalment options for licence renewal fees, and additional support mechanisms for retailers. Further relief was provided through grace periods for selected administrative payments relating to lease contracts, the Registrar of Companies, the Data Protection Department, and the enrolment of employees into the DIFC Employee Workplace Savings ('DEWS') scheme.

You can read the DIFC announcement in full [here](#).

1.4 DFSA Publishes Thematic Review Findings

On 10 April, the DFSA released findings from a thematic review assessing the effectiveness of compliance arrangements across fintech Authorised Firms operating within the DIFC. The review examined a diverse sample of fintech business models, including crowdfunding platforms and money services firms, covering varying organisational sizes and maturity levels.

Key observations included:

- resourcing and staffing constraints
 - 53% of firms operate with three or fewer compliance staff, with some relying on a single individual, which creates significant key person risk and limits operational resilience
- high levels of outsourcing
 - 58% of firms outsource compliance functions
 - in several cases, this resulted in limited local oversight, slower responsiveness, and weaker integration of compliance into day-to-day operations
- governance gaps and dual roles
 - some firms demonstrated insufficient board-level oversight of compliance matters
- reactive compliance culture
 - compliance was sometimes treated as a tick-box exercise, rather than a proactive, embedded component of business strategy
- inconsistent use of technology
 - while 90% of firms reported using compliance technology, the maturity and effectiveness of implementation varied widely
- weak regulatory engagement
 - the DFSA observed delays in notifications, slow responses to supervisory queries, and limited proactive escalation of issues.

The DFSA also outlined several priority areas for strengthening compliance frameworks:

- adequate and proportionate resourcing aligned with business complexity
- stronger governance structures, including clearer oversight by senior management and boards
- embedding a proactive compliance culture across all business lines
- enhanced use of technology and automation to support monitoring and reporting
- timely, transparent, and proactive regulatory engagement with the DFSA.

You can read the findings from the DFSA thematic review in full [here](#).

1.5 DFSA Issues Liquidity Survey

On 10 April, and further to the Dear SEO Letter dated 26 March 2026, the DFSA issued a follow-up communication to Senior Executive Officers ('SEOs') of DFSA-authorized firms. The DFSA requested that all firms authorised to conduct the Financial Service of Managing a Collective Investment Fund report on any liquidity risk management considerations and redemption pressures within their fund structures.

To support this exercise, the DFSA made the Funds Liquidity Survey V1 available on the DFSA ePortal. All Authorised Firms were required to complete the survey by 16 April 2026, regardless of whether they had experienced any liquidity-related issues. The DFSA emphasised that the requirement applied to all firms, including those with no current liquidity concerns.

1.6 DFSA Issues Survey on Marketing and Selling Foreign Funds

On 10 April, the DFSA issued an email to SEOs of DFSA-authorized firms regarding the marketing and selling of Foreign Funds. The notice followed the DFSA's ongoing supervisory focus on firms operating under Article 54 of the Collective Investment Law.

The DFSA confirmed that the requirement applied to all Authorised Firms that market or sell Foreign Funds, irrespective of the scale or nature of their activities. To support this supervisory review, the DFSA made the Marketing and Selling of Foreign Funds Survey V1 available on the DFSA ePortal. All firms were required to complete the survey by 16 April 2026.

1.7 DFSA Issues Revisions to the Business Continuity Measures

On 16 April, the DFSA issued an email communication to all Authorised Firms, DNFBPs, and Representative Offices advising that further amendments have been made to the Business Continuity Measures Form. This update followed the Dear SEO Letter dated 11 March 2026 on the same subject.

The DFSA confirmed that the requirement applied to all Firms, irrespective of whether a previous Business Continuity Plan ('BCP') notifications were submitted. All Firms were required to complete and submit the Business Continuity Measures Form v3 (4/2026) via the DFSA ePortal before 22 April 2026.

1.8 DFSA Issues Two Alerts

On 8 April and 17 April, the DFSA issued two scam alerts highlighting multiple impersonation and advanced-fee fraud schemes targeting the DIFC community. The first alert concerned the misuse of a deceptively similar name, "Nomura Investment International Plc", falsely presented as being associated with the DFSA-authorized firm Nomura International plc (DIFC Branch). Fraudsters circulated fabricated investment documentation, created fake websites and contact details, and sought advance fees under fraudulent investment arrangements. The DFSA confirmed that the entity is not authorised and reminded stakeholders to verify firms through the DFSA Public Register and remain cautious of unsolicited investment approaches.

A subsequent alert on 17 April identified an advanced-fee scam involving impersonation of DFSA-authorized firm FIG Investments Ltd and the DFSA itself. Fraudsters used forged DFSA-branded letterheads, falsified signatures, and a fake email domain (compliance@supportdfsa.net). The DFSA reiterated that Authorised Firms were not permitted to use DFSA-branded stamps or materials and emphasised the need for vigilance regarding communications misusing DFSA branding or an Authorised Firm's details.

In addition, the DFSA issued a public warning via LinkedIn regarding the rise in QR-code-based scams in the UAE, noting increased use of malicious QR codes for phishing, data harvesting, and unauthorised transactions. Firms were urged to enhance staff awareness and strengthen controls around this emerging fraud risk.

You can read the DFSA alerts in full [here](#).

1.9 DIFC Announces AI-Native Financial Centre

On 22 April, the DIFC announced its transition to become an AI-native financial centre, embedding artificial intelligence across its legal, regulatory and operational framework.

The DIFC also outlined key areas of focus for AI integration across its legal, regulatory and operational framework:

- AI to be integrated across legal frameworks, regulatory systems, business operations and infrastructure
- builds on existing AI strategy and inclusion of AI within the DIFC Data Protection Law
- development of AI governance frameworks addressing both human and AI-driven activity
- focus on enabling AI-driven financial services, compliance systems and ecosystem innovation.

The DIFC highlighted the continued integration of AI across regulatory requirements, governance frameworks and operational environments.

You can read the DIFC announcement in full [here](#).

1.10 DFSA Issues Dear Finance Officer Letter on EPRS Reporting Errors

On 23 April, the DFSA notified Authorised Firms via direct email addressed to Finance Officers and Compliance Officers that their Q4 2025 Electronic Prudential Reporting System ('EPRS') returns contained errors or omissions. They were instructed to address these issues in their Q1 2026 submissions and to ensure that all future regulatory reporting is accurate, complete, and compliant with the Prudential – Investment, Insurance Intermediation and Banking Module ('PIB') and Prudential Rules Sourcebook ('PRU') requirements. While the DFSA did not require resubmission of the Q4 returns, Authorised Firms were expected to review their capital and liquidity calculations and enhance their systems and controls to prevent future misreporting.

1.11 DFSA Publishes Summary of Consultation Paper 170

In April, the DFSA issued a summary of Consultation Paper No.170, originally published in March, proposing amendments to the DFSA General Module ('GEN') and Glossary Module ('GLO') Rulebooks.

The proposed updates introduce a new section in GEN Chapter 5 ("Management, Systems and Controls") dedicated to structured operational-resilience framework requiring firms to identify critical business services, set impact tolerances, maintain capabilities to stay within those tolerances during disruptions, and ensure governing-body oversight. The accompanying guidance explains record-keeping expectations, notification duties, and references DFSA supervisory materials.

Under the proposals, Authorised Persons would be required to:

- identify and regularly assess their critical business services
- for each critical business service:
 - o obtain an approval from a governing body of the outcome of the critical business service assessment
 - o set appropriate impact tolerances
 - o map the resources necessary for its delivery
 - o conduct scenario testing to assess the ability to remain within impact tolerances
 - o notify the DFSA of any material disruption that results in, or comes reasonably close to resulting in, a breach of the applicable impact tolerance.

You can read the summary of the Consultation Paper [here](#), and the comments are welcome until 26 May.

Further information

If you have any questions or concerns regarding these DIFC and DFSA developments and requirements, please contact [Nigel Pasea](#).

2. ADGM AND FSRA LATEST DEVELOPMENTS

2.1 ADGM RA Issues Warning

On 6 April, the ADGM's Registration Authority ('RA') and the Financial Services Regulatory Authority ('FSRA') issued an alert warning the public about "Meer Group", noting that it falsely claimed ADGM regulation, promoted unrealistic investment returns, and misrepresented ADGM's role. The regulators clarified that the related ADGM-registered entity is only licensed as a passive holding company and that neither it nor Meer Group is authorised to conduct financial services in or from ADGM.

You can read the ADGM warning in full [here](#).

2.2 FSRA Issues Guidance on Business Risk Assessment

On 10 April, the FSRA published a Dear SEO Letter "Guidance on Business Risk Assessment", setting out regulatory guidance on the preparation and maintenance of Business Risk Assessments.

The guidance reinforces that a documented Business Risk Assessment is both a legal and supervisory requirement and forms the foundation of an effective risk-based Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing ('AML/CTF/CPF') framework. Firms are expected to implement a proportionate, well-documented methodology covering key inherent risk categories, including customer, geographic, product/service, delivery channel, transactional, and emerging technology risks.

Key expectations include board or senior management oversight and approval, an objective assessment of control effectiveness, determination and ongoing monitoring of residual risks, and at least annual reviews or updates triggered by material business or regulatory changes. Firms are reminded that Business Risk Assessment outcomes must be fully integrated into their broader compliance and risk management frameworks.

You can read the Dear SEO Letter in full [here](#).

2.3 FSRA Issues Reminder on 2025 AML Return

On 11 April, the FSRA issued a reminder to Money Laundering Reporting Officers ('MLROs') regarding the upcoming deadline for the submission of the 2025 Annual AML Return (the 'Return'), due by 30 April 2026. The FSRA reiterated that failure to submit the Return by the prescribed deadline would result in a late filing fee and could lead to a referral to enforcement for further action.

The FSRA also reminded that all submissions must be completed via FSRA Connect, noting that login credentials had been previously issued to each firm's registered MLRO. Firms unable to access their credentials were instructed to contact the FSRA immediately to avoid delays.

The communication further clarified that DNFBNPs incorporated or registered in ADGM after 31 October 2025 were not required to submit the 2025 Return.

2.4 FSRA Conducts Virtual Outreach Session on UAE FATF Mutual Evaluation

On 21 April, following an invitation issued on 6 April, the FSRA held a virtual outreach session for SEOs, MLROs, and Principal Representatives ('PRs') to discuss key AML/CFT obligations and the UAE's preparations for the Financial Action Task Force ('FATF') Mutual Evaluation.

The session was organised by the FSRA's Financial & Cyber Crime Prevention ('FCCP') function in cooperation with the AML/CFT General Secretariat. The outreach aimed to reinforce core AML/TFS requirements and provide updates on the UAE's ongoing FATF Mutual Evaluation process.

The key points covered the following:

- core components of the ADGM legislative framework
- overview of the FSRA's AML/TFS regulatory framework and application of FSRA AML Rulebook
- key observations and recommendations
 - o governance and effective AML/TFS policies and procedures
 - o roles of the MLRO, Deputy MLRO and reporting
 - o business risk assessment and customer risk assessment ('CRA')
 - o prohibited relationships
 - o Know Your Customer ('KYC'), due diligence and ongoing monitoring
 - o sanctions compliance
 - o internal and external Suspicious Transaction Reports/Suspicious Activity Reports ('STRs/SARs') and tipping off
 - o co-operation with the regulatory authorities
 - o record keeping and AML/TFS trainings
 - o goAML registration and EOCN alerts
- national coordination
- UAE National Strategy (2024 – 2027).

The UAE's mutual evaluation process began in 2025 with the submission of the Technical Compliance Annex, which sets out the UAE's position against each FATF Recommendation. The UAE also provided its risk, materiality and contextual information to help the assessment team understand the national risk profile and determine the scope of the review. In addition, the UAE submitted its Effectiveness Report covering the 11 Immediate Outcomes, which is currently undergoing iterative feedback and revision.

By the end of May, the authorities will coordinate with the FATF Secretariat to finalise the onsite visit programme. On 6 June 2026, the national team, including private-sector representatives, will participate in training and simulation exercises to prepare for the assessment. The FATF onsite visit will begin on 8 June 2026 and is expected to last between 13 and 16 working days.

The FSRA emphasised that the private sector plays a significant role during the onsite visit, with the assessment team requesting meetings with selected firms based on criteria such as size and sector and potentially adding further entities during the visit. Firms will be expected to demonstrate a clear understanding of their ML/TF/PF risks, compliance obligations, record-keeping practices and alignment with supervisory expectations. The process is rigorous, and any deficiencies identified may affect the UAE's overall ratings, particularly in relation to effectiveness.

The FSRA also shared key expectations for private sector entities in preparation for the FATF onsite visit which focus on demonstration effectiveness in practice as follows:

- AML/CFT manuals must be kept up to date and reflect current UAE laws, regulations, and guidance, as outdated references may indicate weak governance
- the focus should be on effectiveness rather than documentation, with emphasis on how controls operate in practice rather than their existence alone
- firms are expected to demonstrate a clear understanding of UAE ML/TF risks, including the ability to articulate the risk context and apply a risk-based approach
- risk-based approach must be evident, with risk assessments driving decisions and a clear and consistent risk narrative
- sanctions and TFS must be effectively implemented, with immediate action and no uncertainty in application
- remediation actions should be clearly underway, reflecting a continuous improvement approach

- firms must be well-prepared for onsite interviews, providing confident and consistent responses supported by practical examples rather than theoretical explanations
- the onsite visit should be treated as a national responsibility requiring coordinated and constructive engagement across all participants.

2.5 FSRA Publishes Dear SEO Letter

On 24 April, the FSRA published Dear SEO Letter “SSC Joint AML/CFT/CPF Guidance on the CO/MLRO Function in the UAE”, informing firms of the Supervisory Sub-Committee’s Joint Guidance on the AML/CFT/CPF Compliance Officer and Money Laundering Reporting Officer function.

The guidance outlines supervisory expectations and provides practical direction on the governance, appointment, independence, resourcing, and responsibilities of the CO/MLRO roles to support consistent and effective implementation of AML/CFT/CPF requirements across the UAE.

The FSRA reiterated that Relevant Persons are expected to review the guidance and assess the alignment of their existing AML/CFT/CPF frameworks, including the structure and operation of their CO/MLRO function, with the principles and expectations set out therein.

You can read the FSRA Dear SEO Letter in full [here](#).

2.6 ADGM Amends Its Commercial Legislation

On 24 April, the ADGM implemented a series of amendments to its commercial regulations and rules. The updated regulations include:

- Administrative Regulations (Amendment No.1) 2026
- Beneficial Ownership and Control Regulations (Amendment No.1) 2026
- Companies Regulations (Amendment No.1) 2026
- Distributed Ledger Technology Foundations Regulations (Amendment No.1) 2026
- Foundations Regulations (Amendment No.1) 2026
- Trusts (Special Provisions) Regulations (Amendment No.1) 2026.

In addition, the following rules were also issued:

- Commercial Licensing Regulations (Conditions of Licence and Branch Registration) Rules 2026.

You can read the ADGM amended regulations and rules in full [here](#).

2.7 FSRA Implements Enhancements to Insurance Regulatory Framework

On 27 April, the FSRA confirmed the implementation of the proposals outlined in Consultation Paper No. 13 of 2025 “Insurance & Climate-Related Financial Risk Management”, introducing targeted enhancements to ADGM’s insurance regulatory framework and new proportionate requirements for managing climate-related financial risks.

The updates to the insurance framework strengthen insurance risk management, market conduct, and reinsurance practices in line with international standards, operationalise IFRS 17 for ADGM insurers and reinsurers, and introduce various amendments to improve regulatory clarity and remove unnecessary obligations. In addition, all Authorised Persons and Recognised Bodies will now be required to identify, assess, and manage climate-related financial risks where these are material to their business.

The following rulebooks are affected by this update:

- Captive Insurance Business Rulebook (‘CIB’)
 - o deletion of quarterly regulatory return requirement

- changes to cell company reporting requirements
- amendments to submission requirements for EPRS Quarterly Returns
- addition of climate related financial risk ('CRFR')
- updates to reinsurance risk definition
- changes to discount rate rules under IFRS 17
- clarification on accounting standards
- Conduct of Business Rulebook ('COBS')
 - insurers, insurance managers, and insurance intermediaries must identify, prevent, and manage conflicts or potential conflicts of interest to ensure clients are treated fairly
 - implement systems and controls to prevent conflicts from adversely affecting client interests
 - any conflict or potential conflict must be disclosed in writing to affected clients
 - if a conflict cannot be prevented or effectively managed, the firm must decline to act for the affected clients
 - insurers must ensure that new insurance products are developed with proper governance and due diligence, including understanding target client segments, assessment of product characteristics, identifying suitable and unsuitable client segments and oversight of third-party product development
- General Rulebook ('GEN')
 - firms must integrate Climate-Related Financial Risk into their risk management frameworks by assessing materiality (business model and strategy, financial position, ability to meet regulatory obligations) and managing material climate risks
- Glossary Rulebook ('GLO')
- Market Infrastructure Rulebook ('MIR')
- Prudential – Insurance Business Rulebook ('PIN')
- Prudential – Investment, Insurance Intermediation and Banking Rulebook ('PRU')

The amendments came into effect on 27 April 2026.

You can read the FSRA notice in full [here](#).

2.8 FSRA Publishes Updates to Staking Regime

On 29 April, the FSRA issued updates to its rulebooks following the completion of Consultation Paper 10 of 2025 "Proposed regulatory framework for the staking of virtual assets", published in September 2025. The new rules are effective from the date of publication.

The amendments apply across the following rulebooks:

- COBS: a new section added to Chapter 17 ("Additional Rules") dedicated to staking arrangements, including restrictions, the provision of staking services, and permitted methods of delivery
- FUNDS: chapter 3 was updated to clarify that an arrangement does not constitute a fund when it is made by an Authorised Person solely to facilitate the staking of VAs belonging to its clients
- GLO: a definition of "staking" was added.

You can read the FSRA notice in full [here](#).

2.9 FSRA Issues Two Regulatory Alerts

On 14 April, the FSRA issued a regulatory alert warning the market and the public about misleading claims made by an entity calling itself "MaskEx". The FSRA confirmed that MaskEx falsely claimed to hold an ADGM licence and to be registered in multiple jurisdictions, including displaying a fabricated "ADGM Category 3C Money Services Business Licence" on its website. The FSRA clarified that MaskEx was never licensed, authorised, or incorporated in ADGM, and advised investors to verify authorisations through the FSRA Public Register before dealing with any firm.

On 28 April, the FSRA issued another warning in relation to two websites (exinityxe.cc and exinityx.com) which closely imitate the official website of Exinity ME Ltd (trading as Nemo), an FSRA-regulated entity.

The FSRA confirmed that these websites are not associated with Exinity and that their operators are not licensed or authorised to conduct regulated activities in or from ADGM.

The FSRA encouraged individuals to report concerns relating to fraudulent financial services websites through its Complaints Portal. Guidance on reporting cybercrime to the relevant authorities is also available via the links provided by the FSRA.

You can read the FSRA alert in full [here](#) and [here](#).

2.10 FSRA Issues Consultation Paper on AML Framework Enhancements

On 30 April, the FSRA issued Consultation Paper No. 1 of 2026, proposing targeted enhancements to its AML, CTF, CPF, and sanctions compliance framework.

The proposed amendments update the Financial Services and Markets Regulations 2015 ('FSMR') and the AML and Sanctions Rulebook ('AML') to reflect developments in the UAE federal legislation and align with evolving international standards, including FATF recommendations.

The AML Framework applies to Authorised Persons, Recognised Bodies, DNFBPs and Non-Profit Organisations ('NPOs'). FSRA noted that the changes were largely incremental and were expected to have minimal impact on existing compliance obligations. The consultation also includes miscellaneous amendments to the GEN, GLO, and Guidance and Policies Manual.

You can read the consultation paper in full [here](#) and comments were welcome until 14 May.

2.11 FSRA Issues Cyber Threat Notice for VASPs

On 30 April, the FSRA issued a notice highlighting key cyber threats relevant to Virtual Asset Service Providers ('VASPs'). The notice reflects an observed increase in the sophistication and scale of cybercrime targeting virtual asset ecosystems and outlines risks such as private key compromise, ransomware and extortion, deepfake-enabled identity fraud, supply chain attacks, and decentralised finance ('DeFi') exploits.

FSRA reminded firms to ensure their cybercrime prevention and resilience frameworks remain risk-based, proportionate, and regularly reviewed, taking into account emerging threats, including AI-driven attacks and longer-term quantum risks. The notice also reiterates regulatory expectations around strong key custody arrangements, secure-by-design systems, effective third-party risk management, staff awareness, and incident response readiness.

Firms remain subject to the requirement under GEN 3.5 to report material IT or cyber incidents to FSRA within 24 hours of discovery.

You can read the FSRA Dear SEO Letter in full [here](#).

Further information

If you have any questions or concerns regarding these ADGM and FSRA developments and requirements, please contact [Shadi Dajani](#).

3. MIDDLE EAST REGULATORY UPDATES

3.1 CMA Issues Request for Economic Impact Assessment

On 8 April, the Capital Market Authority ('CMA' or the 'Authority') issued an email notification requesting all CMA-regulated firms to assess and report the direct and indirect economic impact of the current regional circumstances on their business. Firms were instructed to complete the CMA's assessment template, upload the required supporting documentation, and submit the information by 8 April 2026.

The CMA noted that the exercise forms part of its ongoing monitoring of the effects on regulated entities and the broader UAE capital markets sector. The Authority also confirmed that all information submitted will remain confidential and used solely for official purposes.

3.2 UAE Authorities Revise Administrative Tax Penalties

On 14 April, UAE Cabinet Decision No. 129 of 2025 introduced amendments to the administrative penalties regime applicable to violations of UAE tax laws, including VAT, Excise Tax, and Corporate Tax. The Decision, issued in October 2025 and published on 10 November 2025, forms part of the UAE's broader initiative to strengthen tax compliance, enhance consistency, and improve transparency across the national tax framework.

Key provisions include:

- introduction of revised administrative penalties applicable to breaches of the Tax Procedures Law, VAT Law and Excise Tax Law
- introduction of a 14% annualised monthly penalty on unpaid Payable Tax, replacing the previous multi-tier late payment structure
- introduction of a 1% monthly penalty on the Tax Difference arising from voluntary disclosures until submission
- introductions of a 15% fixed penalty where voluntary disclosure is submitted after notification of a tax audit
- reduction of penalties for certain administrative breaches including failure to update tax records, failure to notify appointment of a legal representative and incorrect tax returns
- introduction of specific penalties for failure to issue tax invoices or tax credit notes within the legally prescribed timeframe
- confirmation penalties apply across violations covering Tax Procedures Law, VAT and Excise Tax obligations.

The amendments revise the administrative penalties framework applicable to UAE federal tax legislation by updating penalty amounts, introducing percentage-based penalties applicable to late payment and voluntary disclosures, and clarifying penalties applicable to key compliance obligations including tax filings, record keeping and invoicing requirements.

You can read the Cabinet Decision No.129 in full [here](#).

3.3 CMA Issues Dear CEO Letter on Key AML/CFT/CPF Obligations

On 14 April, the CMA issued a Dear CEO Letter "Key AML/CFT/CPF Obligations, Emerging Risks and Supervisory Observations for Securities Firms and VASPs, 2025," summarising findings from the 2025 supervisory engagement cycle and risk assessment, including onsite inspections, review of MLRO reports, thematic reviews and desk-based reviews.

The CMA's supervisory work identified several recurring deficiencies and common areas of weakness, suggesting broader compliance challenges across segments of the securities sector. These insights have directly informed the CMA's supervisory priorities, subsequent follow-up actions, and the development of wider risk-mitigation measures.

Key deficiencies affected the following areas:

- risk appetite framework
 - o lack of clear risk appetite criteria
 - o weak financial crime key risk indicators
 - o poor linkage between risk assessment and risk appetite
- regulatory gap analysis and alignment
 - o absence of formal regulatory gap analysis
 - o weak regulatory change management processes
 - o insufficient integration of national and sectoral risk assessments
- customer risk assessment methodology
 - o lack of differentiation in customer risk assessment
 - o missing key customer risk factors
 - o misalignment with regulatory risk guidance
- internal and external audit
 - o inadequate internal audit focus and independence
 - o limited audit coverage of financial crime controls
 - o weak assurance frameworks leading to undetected deficiencies
- training needs
 - o lack of comprehensive training needs analysis
 - o training not tailored to employee roles and risk exposure
- MLRO governance and deputy arrangements
 - o no defined MLRO continuity or coverage arrangements
 - o gaps in succession and delegation planning
 - o undefined eligibility and independence requirements for deputy MLROs
- management information, key performance indicators ('KPIs') and key risk indicators ('KRIs')
 - o absence of a dedicated financial crime KPI/KRI framework
 - o inadequate management information systems for financial crime reporting
 - o limited ability to monitor trends and identify control weaknesses.

Key emerging risks specific to VASPs are as follows:

- P2P transaction risks and disintermediation
 - o reduced transparency and bypassing of regulated channels
 - o increased anonymity and exposure to illicit activity
- use of unregulated or offshore virtual asset platforms
- wallet-to-wallet transfers and limited traceability
- rapid movement of funds and velocity risks
- sanctions evasion and typologies
- reliance on third-party technology and blockchain analytics
- inadequate risk assessment integration.

CMA expects Financial Institutions, including those engaging directly or indirectly with virtual asset activities to:

- identify and assess of virtual asset and P2P risks
- apply enhanced due diligence for Virtual Assets ('VAs') and P2P exposure
- implement robust transaction monitoring and blockchain analytics
- implement effective sanctions screening for VAs
- have policies for engagement with VASPs
- have governance and board oversight of VA risks
- regularly update controls to meet regulatory expectations
- manage cross-border VAs transfers and high-risk counterparties.

The CMA emphasised that it would take supervisory or regulatory action when necessary to address inadequate compliance arrangements, in order to protect the integrity of the financial system. At the same time, it will continue providing guidance and engaging with the sector to help institutions meet their obligations and strengthen a culture of compliance, vigilance, and effective financial crime risk management.

3.4 CBUAE Launches Unified e-KYC Platform

On 15 April, the Central Bank of the United Arab Emirates ('CBUAE') announced the development of a nationwide unified e-KYC platform. The initiative forms part of CBUAE's financial infrastructure transformation programme and aims to modernise KYC and due diligence processes across the UAE financial sector.

The e-KYC platform will streamline KYC and know your business processes through automated workflows and trusted data integration, reducing duplication, compliance costs, and onboarding timelines

You can read the CBUAE announcement in full [here](#).

3.5 CBUAE Updates AML/CFT/CPF Guidance

On 16 April, the CBUAE issued an updated package of AML/CFT/CPF guidance and best-practice manuals to strengthen the effectiveness of financial crime risk management frameworks across Licensed Financial Institutions and Registered Hawala Providers. The guidance aligns with FATF standards and the UAE National AML/CFT Strategy 2024 - 2027.

The package includes the following guidance documents:

- risks related to proliferation financing
 - o outlines expectations for assessing, mitigating, and monitoring proliferation financing risks through robust CPF frameworks and ongoing identification of emerging risks
- risks related to trade-based money laundering and transshipment
 - o focuses on developing a deeper understanding of money laundering, terrorist financing and PF risks associated with trade and transshipment
- correspondent banking and expectations for managing correspondent banking relationships
 - o sets out guidance for institutions providing these services in formulating internal policies and procedures that comply with the UAE's legal frameworks, ensuring their operations align with the new guidance for effectively managing risks arising from correspondent banking relationships
- customer due diligence ('CDD'), KYC requirements, and record keeping
 - o outlines the core principles that supervised institutions must consider when building a customer risk profile, clarifying simplified and enhanced due diligence procedures, and specifying the types of data and documentation that must be retained on record.

In addition, the CBUAE published two best-practice manuals in relation to:

- implementing a risk-based approach and conducting risk-based institutional risk assessments
- implementing role-based training on AML/CFT/CPF.

You can read the CBUAE guidance documents in full [here](#).

3.6 SSC Issues Guidance on CO/MLRO Function

On 24 April, the UAE Supervisory Sub-Committee ('SSC') issued guidance for the CO and MLRO functions across Financial Institutions, DNFBPs and VASPs.

The guidance reinforces the CO/MLRO role as a central pillar of the AML/CFT/CPF framework, aligned to Federal Decree Law No. 10 of 2025 and Cabinet Resolution No. 134 of 2025, and consistent with FATF standards.

Key regulatory expectations were:

- appointment of a senior, independent CO/MLRO with sufficient authority and direct access to the board
- clear accountability of the CO/MLRO for oversight of the AML/CFT/CPF framework, including transaction monitoring, suspicious activity reporting and business risk assessments
- designation of the CO/MLRO as the primary point of contact with regulators and the financial intelligence unit
- establishment of a compliance function that is adequately resourced, skilled and proportionate to the firm's risk exposure
- the CO/MLRO role and key compliance functions to be carried out internally, with only limited AML tasks eligible for outsourcing subject to regulatory approval
- implementation of formalised semi-annual reporting by the CO/MLRO to senior management and supervisory authorities.

Key recurring deficiencies identified were:

- insufficient seniority and independence of the CO/MLRO
- weak governance frameworks and limited board engagement
- over-reliance on group or third-party compliance arrangements
- inadequate involvement of the CO/MLRO in key control decisions, including transaction monitoring, sanctions and CDD
- gaps in the design and execution of risk-based AML/CFT/CPF programmes.

Key requirements for firms include:

- strengthening CO/MLRO independence, authority and reporting lines
- enhancing resourcing and capability within compliance functions
- ensuring local ownership and oversight of AML/CFT/CPF controls
- embedding effective board engagement and challenge across financial crime risks.

You can read the SSC guidance in full [here](#).

3.7 CMA and FIU Hold Awareness Session on Reporting

On 29 April, the CMA and the UAE Financial Intelligence Unit ('UAEFIU') held a virtual awareness session on the effectiveness of suspicious reporting. The session focused on enhancing understanding of effective suspicious transaction reporting practices, improving reporting quality and internal controls, and providing an overview of STR/SAR statistics and strategic insights. The authorities emphasised that reporting entities play a critical role in supporting the national AML/CFT framework, noting that effectiveness is driven by the quality, clarity and timeliness of submissions rather than the volume of reports filed.

Key common reporting deficiencies to avoid include:

- weak or generic narratives (e.g., reliance on attachments without explanation)
- incorrect reason for reporting ('RFR') selection
- incomplete or inconsistent supporting documentation
- limited linkage between transactional activity and external intelligence
- insufficient analytical depth in reports.

The session also set out regulatory expectations for a shift towards intelligence-led reporting, requiring firms to demonstrate enhanced analytical capability and clear articulation of suspicion within their reporting, including:

- suspicion must be clearly defined and supported by behavioral, structural, geographic or economic indicators
- reporting must move beyond factual descriptions and provide structured, analytical narratives explaining why the activity is suspicious

- all submissions, including suspicious transaction reports, suspicious activity reports and additional information files, must be routed through goAML or IEMS
- reports must include complete and relevant supporting documentation, including KYC records, account activity and enhanced due diligence materials
- adverse media should be used to support and contextualise transaction analysis, rather than forming the sole basis of suspicion
- strict confidentiality must be maintained throughout the reporting lifecycle to mitigate tipping-off risks
- firms are expected to maintain ongoing engagement with the FIU, including submission of additional information files where new findings arise.

The session also presented a case study in which a reporting entity identified a customer misrepresenting themselves as a real estate agent to facilitate fraud, submitted a suspicious transaction report and used the goAML message board to request prioritisation. As a result, the FIU, in coordination with counterpart FIU's and law enforcement authorities, issued a freeze order, resulting in the recovery of over AED 6Mn in criminal proceeds. This highlights the critical importance of proactive identification, high-quality reporting, and effective engagement with regulatory and enforcement channels in mitigating financial crime risk.

3.8 CMA Issues VASP and ATS Regulations

In April, the CMA published the English versions of the regulatory framework pursuant to the Chairman of the Authority's Board of Directors' Resolution No. (04/Chairman) of 2026, governing Virtual Asset Service Providers ('VASPs'), comprising the General Framework Module, Alternative Trading System ('ATS') Module and Business Regulation Module, establishing licensing, conduct of business and market infrastructure requirements for virtual asset activities conducted in or from within the UAE.

Key provisions of the General Framework Module include:

- introducing a licensing regime for virtual asset activities including dealing, custody, arranging, portfolio management, advice and operating multilateral trading facilities
- prohibiting financial services relating to privacy tokens and algorithmic tokens, and restricting activities relating to utility tokens and non-fungible tokens ('NFTs') without prior approval
- introducing a virtual asset registration framework and "Green List" mechanism for recognised virtual assets
- establishing governance, systems and controls, risk management, cybersecurity and outsourcing requirements for licensed entities
- introducing approval and notification requirements relating to controllers, ownership changes and regulatory reporting.

Key provisions of the ATS Module include:

- establishing a licensing and in-principle approval regime for operators of ATS, including Multilateral Trading Facilities ('MTFs') and Organised Trading Facilities ('OTFs')
- introducing requirements relating to governance, organisational structure, key persons, conflicts of interest management, operational resilience and technology controls
- establishing market conduct and infrastructure requirements including admission standards, transparency, transaction recording, custody arrangements and market abuse prevention controls
- introducing additional requirements for trading venues dealing in tokenised securities, tokenised commodities and virtual assets, including technology audit, disclosure and white paper requirements.

Key provisions of the Business Regulation Module include:

- introducing conduct of business requirements including AML/CTF compliance, client classification (retail, professional and counterparty) and client agreement requirements
- introducing suitability and appropriateness assessment requirements and recordkeeping obligations
- establishing conflicts of interest, inducement and fair client treatment requirements
- introducing detailed client asset and client fund protection requirements including custody, segregation and reconciliation controls

- introducing requirements relating to margin trading, lending and borrowing, staking, digital wallet services and disclosure of virtual asset risks including white papers and key characteristics documents.

You can read the CMA regulations in full [here](#).

3.9 CMA Launches Open Data Portal

In April, the CMA launched an open data portal on its website through which stakeholders may submit requests for access to regulatory and market data, supporting transparency and data accessibility.

You can access the open data portal on the CMA website [here](#).

3.10 CMA and UASA Deliver Professional Development Programmes

In April, the CMA and the Union of Arab Securities Authorities ('UASA') announced a series of structured continuous professional development ('CPD') programmes aimed at enhancing regulatory knowledge and supervisory capabilities across the region. The courses will be delivered throughout May and June.

The UASA was established in 2007 and is a non-profit organisation dedicated to supporting the development of Arab securities and derivatives regulators. Its mandate includes advancing legislative and regulatory frameworks to promote fairness, efficiency, and transparency across securities markets.

The CPD courses cover the following topics:

- detecting financial crimes in citizenship and residency by investment programs (FATF Requirement)
- introduction to fintech and innovation
- ESG and money laundering risks
- AML, risk-based approach, and beneficial ownership transparency
- climate change risk in financial institutions
- financial crimes and crypto assets
- derivatives
- professional technical analysis.

You can access the UASA website [here](#) and the CMA CPD requirements [here](#).

3.11 CMA Issues Several Warnings

Throughout April, the CMA issued several warnings advising investors to avoid dealing with multiple unlicensed entities, including Allegiant Metals Group, Fundfloat Academy, YA Group Ltd, NXG Markets, and Better Experience. The regulator also clarified that Naqdi Securities Currencies Brokers LLC is licensed only for investment introduction and financial advisory, and any additional services promoted through its website or social media are unauthorised. Investors are urged to verify licensing status before engaging with any entity to protect against potential fraud.

You can read the CMA warnings [here](#).

Further information

For any questions or concerns regarding these updates, please contact [Mohsin Ismail](#).

4. INTERNATIONAL UPDATES

4.1 UNSC Updates Sanctions List

The UN Security Council ('UNSC') issued several updates to its sanction lists on 13, 15, and 29 April amending a total of 28 entries.

On 13 and 15 April, the UNSC established pursuant to resolution 1988 (2011) enacted three and four amendments, respectively, to the entries on its 1988 List of individuals and entities subject to the assets freeze, travel ban, and arms embargo set out in paragraph 1 of Security Council resolution 2816 (2023), adopted under Chapter VII of the Charter of the United Nations.

On 28 April, the UNSC issued two updates to its Sanctions List, pursuant to resolution 1591 (2005) concerning the Sudan addition of four entries, and seventeen entries pursuant to resolution 1988 (2011) subject to the measures imposed by the Security Council and adopted under Chapter VII of the Charter of the United Nations.

You can read the amended entries to the sanctions list [here](#), [here](#), [here](#), and [here](#).

4.2 FATF Holds Ministerial Meeting

On 17 April, Ministers from jurisdictions worldwide have reaffirmed their collective commitment to combating illicit finance through enhanced multilateral cooperation under the FATF. During the biennial FATF Ministerial Meeting, held alongside the International Monetary Fund ('IMF') World Bank Spring Meetings, Ministers agreed to intensify efforts to address the escalating threat of fraud and to reinforce the effective, risk-based implementation of the FATF Standards.

Ministers highlighted the significant harm caused by illicit financial activity, noting its corrosive impact on national and international security, institutional integrity, economic growth, and sustainable development. They underscored that many countries continue to face severe terrorist attacks and ongoing risks posed by global proliferation networks. In this context, Ministers reiterated that robust action to counter money laundering, terrorist financing, and proliferation financing ('AML/CFT/PF') remains an urgent global priority.

Recognising the rapid expansion of fraud in scale and sophistication, Ministers committed to leveraging the full AML/CFT/CPF framework to disrupt and deter fraudulent activity. They emphasised the need to deepen global understanding of fraud typologies, including organised scam operations and the misuse of legal persons, virtual assets, and emerging technologies such as artificial intelligence.

To ensure that public and private sector resources are directed to the areas of highest risk, Ministers reaffirmed their support for the full and effective implementation of the risk-based approach, which remains central to the FATF Standards. This commitment aims to enhance the strategic allocation of supervisory, enforcement, and compliance efforts across jurisdictions.

The UAE was represented by the Middle East and North Africa Financial Action Task Force ('MENAFATF').

You can read the FATF Ministerial Declaration in full [here](#).

4.3 World Alliance Releases 2026 Report on Artificial Intelligence in Financial Services

On 21 April, the World Alliance of International Financial Centers ('WAIFC') and ADGM have jointly published a new report examining the accelerating adoption of Artificial Intelligence ('AI') across global financial centres and the corresponding need for coordinated, responsible governance. The report is based on a survey of 12 member jurisdictions and focuses on AI's impact on financial services, regulatory considerations, talent development, ecosystem innovation, and associated risks.

The WAIFC is a non-profit association that promotes collaboration among global financial centers to foster innovation and best practices in the financial industry.

Key findings from the report are following:

- AI adoption is now widespread across International Financial Centres ('IFCs'), particularly in compliance, fraud detection, customer service, and portfolio management
- generative AI is significantly enhancing compliance functions through faster, more accurate, and cost-efficient processes, including real-time monitoring
- regulatory frameworks for AI remain uneven, with most jurisdictions relying on general data protection laws and only a few introducing AI-specific regulation
- gaps exist in areas such as accountability for AI-driven breaches, autonomous decision-making, and model transparency
- key risks identified include algorithmic bias, data privacy concerns, reliance on third-party providers, and limited explainability of AI models
- financial institutions are strengthening governance frameworks, including human-in-the-loop controls, to maintain oversight and trust
- AI is reshaping workforce roles, with new positions emerging in AI governance and ethics, though a global talent shortage remains
- IFCs are supporting innovation through regulatory sandboxes, incubators, and targeted funding initiatives
- collaboration among regulators, financial institutions, fintechs, and academia is essential to support responsible AI development
- continued international cooperation is needed to enhance regulatory clarity, address talent gaps, and ensure ethical and resilient AI deployment.

You can read the WAIFC report in full [here](#).

4.4 MENAFATF Chairs Joint Supervisory Authorities Forum

On 23 April, the MENAFATF chaired the Joint Forum of Supervisory Authorities and the Private Sector held in Russia.

The event was organised in cooperation with the Eurasian Group on Combating Money Laundering and Financing of Terrorism ('EAG'), the Eastern and Southern Africa Anti-Money Laundering Group ('ESAAMLG'), and the Intergovernmental Action Group against Money Laundering in West Africa ('GIABA').

The following strategic topics were discussed during the forum:

- rapid evolution of modern technologies and their impact on the financial crime risk environment
- role of digital banks and artificial intelligence in the financial sector
- challenges associated with virtual assets and terrorist financing
- achieving regulatory balance in supervising DNFBPs
- importance of international cooperation in ensuring effective and sustainable financial crime prevention systems.

You can read the MENAFATF announcement in full [here](#).

Further information

For any questions or concerns regarding these updates, please contact [Mohsin Ismail](#).

ABOUT WAYSTONE COMPLIANCE SOLUTIONS

Waystone Compliance Solutions offers a new and unique approach to compliance services at a corporate level.

As a truly global partner, we have the capabilities to help you manage regulatory risk right across your organisation.

We can provide key services from initial registration and licensing to compliance programme integration. Our compliance solutions span business strategies, market activities, and operational and technology infrastructure, not to mention sales and marketing procedures. And we can do so anywhere in the world.

Our aim at Waystone is simple: to enable our clients to navigate the complex regulatory environment with confidence.

At Waystone, we have brought together the experience, the expertise, and the global reach to give you the certainty you need to address the ever-changing regulatory world. And by doing so, provide you with a secure route on the road to success.

<https://compliance.waystone.com/>

Consultancy Services & Support

- Compliance Advisory
 - o The Virtual Compliance Clinic
 - o Assurance Reviews
 - o Compliance Remediation
 - o Data Protection
 - o Financial Crime Prevention
 - o Corporate Governance
 - o Risk Management
 - o Prudential Rules & Regulatory Reporting
- Authorisation
- Outsourcing (Compliance Officer, MLRO, Finance Officer and Data Protection Officer)
- Documentation
- Training

If you wish to discuss how Waystone can assist you with any of the issues raised in this regulatory update, please contact us using the details below:

Email: compliancesolutions@waystone.com

Website: <https://compliance.waystone.com/>

Tel: Dubai +971 4 323 0800 | Abu Dhabi +971 2 440 2146

or write to us at:

Waystone Compliance Solutions
Level 1, Gate Village Building 1,
Dubai International Financial Centre (DIFC),
Dubai, PO Box 506733,
United Arab Emirates

This regulatory update provides information about the consultative documents and publications issued by various regulators which are still current, proposed changes to the Rules and Guidance set out in Handbooks, actual changes to Rules and Guidance that have occurred in the months leading up to the update and other matters of relevance to regulated firms. This regulatory update is intended to provide general summarised guidance only, and no action should be taken in reliance on it without specific reference to the regulators' document referred to therein.