



# Regulatory Update

Middle East, April 2025

Issued 6 May 2025



## Table of Contents

<b>1. DIFC AND DFSA LATEST DEVELOPMENTS .....</b>	<b>3</b>
1.1 DFSA Issues Several Scam Alerts.....	3
1.2 DFSA Holds Digital Assets Regulation Workshop .....	4
1.3 DFSA Issues Dear SEO Letter .....	4
1.4 DFSA and UASA Lead Regional Discussion.....	5
1.5 Dubai AI Festival .....	5
1.6 Dubai World Insurance Congress .....	5
1.7 DFSA Issues Dear SEO Letter .....	5
1.8 DFSA Issues Dear SEO Letter .....	6
1.9 DIFC Data Protection Regulation 10 Workshop .....	6
1.10 DIFC to Host FinTech Summit .....	7
<b>2. ADGM AND FSRA LATEST DEVELOPMENTS .....</b>	<b>7</b>
2.1 ADGM Online Registry for FATCA and CRS.....	8
2.2 FSRA Issues Consultation Paper on Prudential Framework .....	8
2.3 FSRA Issues Multiple Alerts .....	8
2.4 FSRA Issues Dear SEO Letter on Cybercrime Prevention .....	9
2.5 FSRA Issues Dear SEO Letter on Whistleblowing .....	10
2.6 FSRA Publishes Business Plan .....	10
2.7 FSRA Supervision Outreach Session .....	11
2.8 FSRA Issues Consultation Paper on Cyber Risk.....	12
<b>3. MIDDLE EAST REGULATORY UPDATES .....</b>	<b>13</b>
3.1 CMA Adopts New Enforcement Mechanism for AML/CFT Violations .....	13
3.2 UAE Hosts First FATF Global Network Secretariats Roundtable.....	13
3.3 CBUAE Signs MoU.....	13
3.4 UAE Completes National Risk Assessment on AML/CFT .....	13
3.5 UAE Hosts Summit on the Role of DNFBPs in Combating Financial Crime.....	14
3.6 VARA Issues Consumer and Marketplace Alert .....	14
3.7 SCA Issues Several Warnings.....	14
<b>4. INTERNATIONAL UPDATES.....</b>	<b>15</b>
4.1 FATF Updates Consolidated Ratings.....	15
<b>5. ENFORCEMENT ACTIONS.....</b>	<b>16</b>
5.1 FSRA Imposes Fines.....	16
5.2 ADGM RA Imposes Fines.....	16
5.3 CBUAE Imposes Financial Sanction on Bank .....	17
<b>ABOUT WAYSTONE COMPLIANCE SOLUTIONS .....</b>	<b>17</b>

## 1. DIFC AND DFSA LATEST DEVELOPMENTS

### 1.1 DFSA Issues Several Scam Alerts

On 4 April 2025, the DFSA issued a public alert regarding a scam involving the impersonation of CGL (Dubai) Limited, a DFSA-authorized firm.

The fraudsters have created a fake website, [cgl-limited.net](http://cgl-limited.net), which falsely claims to offer trading services through a platform, using the name of CGL (Dubai) Limited without permission. The scammers pressure victims to make additional deposits and increase turnover before allowing withdrawals and communicate with victims via video calls and messages, using multiple international phone numbers.

The DFSA advises the public to:

- avoid visiting the fraudulent website or responding to any communications related to the scam
- not send or provide any money to those involved in the scam

The DFSA encourages consumers to verify the authenticity of firms by consulting the DFSA Public Register and reviewing its alerts page for additional scam warnings and guidance on how to avoid being scammed.

You can read the DFSA alert [here](#).

On 18 April, the DFSA issued a public alert regarding recent fraudulent schemes in which the DFSA and another government organisation in the United Arab Emirates ('UAE'), have been impersonated in fake documents.

The fake documents used by the scammers consisted of:

- a "Fund Release Order/Title Form A" naming an individual with an address in Abuja, Nigeria, and falsely authorising the release of US\$ 82,600,000
- a falsified "Tax Domicile Certificate for Individuals"
- several counterfeit receipts purporting to be issued by a UAE government organisation
- misuse of official logos belonging to the DFSA and a UAE government entity
- unauthorised use of the name "DUBAI FINANCIAL SERVICES AUTHORITY"
- references to a non-existent DFSA "Dubai Regional Office"
- an incorrect DFSA office address and P.O. Box number
- a fake Tax Domicile certification and stamp attributed to a UAE government organisation.

The DFSA asks for the public to be aware that:

- the DFSA does not issue or certify the release of funds for firms or individuals
- the DFSA does not have a "Dubai Regional Office"
- the DFSA's logo, name and other details have been used without permission.

The DFSA urges the public to avoid engaging with the scam and warns against sending any money to those involved.

You can read the DFSA alert [here](#).

On 18 April, the DFSA issued a public alert regarding recent fraudulent schemes in which the DFSA has been impersonated. Scammers are circulating an "Official Notice" falsely claiming to be from the DFSA, requesting a fee to link a bank account to "the transit financial corridor in Dubai" to receive cryptocurrency investment profits. The letter is fraudulently signed by a fake DFSA employee and unlawfully uses logos and stamps from various Dubai authorities.

The DFSA asks for the public to be aware that:

- the "Official Notice" is fraudulent and was not sent by the DFSA

- the DFSA does not require advance fees to release profits of investments
- the DFSA does not establish connections between bank accounts and financial corridors in Dubai.

You can read the DFSA alert [here](#).

On 25 April, the DFSA issued a public alert regarding a scam in which a fake DFSA letter is being used to deceive victims. The scam involves a cryptocurrency trading platform, “Bitget Capital,” which is not authorised by the DFSA or based in the DIFC. Victims are encouraged to create accounts on the platform and, when attempting to withdraw profits, they receive a fraudulent document titled “Notification.”

The fake document includes:

- a fake notification number not generated by the DFSA
- a falsified signature of the DFSA Chief Executive and Chairman
- a statement claiming the DFSA identified irregularities and potential regulatory breaches in victims' accounts
- a claim that the victims' accounts have been frozen
- a request to submit the document to a bank in Singapore to release their funds.

The DFSA has confirmed that this document is not issued by the authority and that the DFSA's logo, name, and other details have been used without permission.

The DFSA urges the public to avoid responding to any communications related to this scam and to refrain from sending money to any parties connected to it.

You can read the DFSA alert [here](#).

## 1.2 DFSA Holds Digital Assets Regulation Workshop

On 10 April, the DFSA hosted a workshop on navigating digital assets regulation, following the introduction of its regulatory frameworks for Investment Tokens in 2021 and Crypto Tokens in 2022, aimed at providing clarity for firms operating in or from the DIFC. These frameworks continue to evolve in line with shifting market dynamics and emerging international standards.

The key areas of discussion were as follows:

- overview of the DFSA's regulatory approach to digital assets, including recent updates
- introduction to the DFSA's Tokenisation Regulatory Sandbox and its role in supporting innovation
- digital asset developments in the DIFC and globally, with key trends, opportunities, and regulatory considerations.

## 1.3 DFSA Issues Dear SEO Letter

On 10 April 2025, the DFSA issued a Dear SEO Letter titled “Reporting Obligations to the DFSA and Fixed Penalty Notices”, reminding firms of their regulatory reporting obligations and the Fixed Penalty Notice (‘FPN’) regime, which has been in effect since 15 April 2024. Timely submission of regulatory reports is critical for effective oversight.

Under the FPN regime, penalties for late or missed submissions are as follows:

- First contravention: US\$ 2,500
- Second contravention: US\$ 7,500
- Third and subsequent contraventions: US\$ 15,000

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

## 1.4 DFSA and UASA Lead Regional Discussion

On 23 April, the DFSA and Union of Arab Securities Authorities ('UASA') held a high-level regulatory insights session centred on fostering innovation in the region. This session brought together senior representatives from the capital market and financial regulatory authorities to explore challenges, opportunities and regulatory approaches in the financial services sector.

You can read the DFSA article [here](#).

## 1.5 Dubai AI Festival

On 23 - 24 April, the second edition of the Dubai AI Festival took place with the overarching theme of "Enabling Digital Economy". This was organised by the Dubai AI Campus in partnership with the DIFC, the Minister of State for Artificial Intelligence, and the Digital Economy and Remote Work Applications Office. The event explored AI's transformative impact across industries, highlighting key advancements, investment opportunities, and the regulatory frameworks shaping the future of AI.

Key themes for 2025 include:

- exploring how AI is driving efficiency, growth, and innovation across industries
- promoting AI literacy and equipping leaders with the skills needed to succeed in an AI-driven world
- highlighting how strategic investments in AI infrastructure can support sustainable, long-term innovation
- showcasing AI's potential to create a more inclusive and accessible future for all
- emphasizing the importance of global AI governance to ensure ethical, secure, and coordinated development
- demonstrating real-world AI applications through immersive, interactive experiences
- balancing innovation and ethics by advancing AI responsibly and sustainably
- examining how automation is transforming the workforce and unlocking human potential.

You can read the DIFC article [here](#).

## 1.6 Dubai World Insurance Congress

On 28 - 30 April, the 8<sup>th</sup> edition of the Dubai World Insurance Congress ('DWIC') was held by Global Reinsurance in partnership with the DIFC. This is the leading industry event for the Middle East, Africa, and South Asia, bringing together senior insurance and reinsurance executives to network and explore emerging opportunities and challenges shaping the future of the sector.

Key discussion topics at this year's congress included:

- future of finance
- global economic trends
- blockchain and cryptocurrency
- financial innovation
- regulatory compliance
- investment outlook
- real estate tokenisation.

You can read the DIFC article [here](#).

## 1.7 DFSA Issues Dear SEO Letter

On 28 April 2025, the DFSA issued a Dear SEO Letter “Newly Authorised Firms Engagement 2025” announcing the launch of engagement sessions in June 2025 for newly Authorised Firms in the DIFC. This initiative responds to the continued growth and interest in the centre. The sessions aim to help firms establish strong compliance foundations and gain a clear understanding of DFSA regulatory requirements from the outset, thereby reducing risks and associated remediation costs.

Key topics will include:

- conduct
- prudential and AML requirements
- operational resilience
- cyber risk
- market risk.

Selected firms will receive invitations in Q2 2025 and may submit questions in advance. A feedback survey will follow to inform future sessions.

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

## 1.8 DFSA Issues Dear SEO Letter

On 28 April 2025, the DFSA issued a Dear SEO Letter titled “Thematic Review on Compliance arrangements 2025” to announce an upcoming thematic review focused on the compliance arrangements of Authorised Firms operating with Money Services (‘MS’) and Crowdfunding Platform (‘CFP’) permissions. The purpose of the review is to assess the effectiveness of current compliance frameworks and identify both good practices and areas needing improvement.

The review will focus on following key areas:

- capacity and resources
- governance and controls
- policies and procedures
- people and culture
- technology and tools
- regulatory engagement.

The review will be conducted in two phases. Phase 1 will require all MS providers and CFP operators to complete a survey outlining their compliance practices, while phase 2, beginning in the second half of 2025, will involve a more detailed review of a selected subset of firms, potentially including on-site visits.

The DFSA emphasised that the proposals outlined in Consultation Paper No.165, “Proposed Changes to the DFSA’s Approach to Licensed Functions and Authorised Individuals,” should not affect the way Authorised Firms respond to this survey.

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

## 1.9 DIFC Data Protection Regulation 10 Workshop

On 29 April, the DIFC held a workshop titled ‘Introduction to the DIFC Regulation 10 Accelerator’, which provided valuable insights and offered a clear understanding of the DIFC’s expectations.

The session introduced the DIFC Data Protection Regulation 10 Accelerator, designed to foster positive AI adoption in line with regional ethical values and largely based on the EU AI Act. AI accelerator is a sandbox where AI systems can be tested against privacy by design and Regulation 10 requirements. The session acted

as a soft launch aiming to gather feedback as AI evolves, focusing on a less burdensome certification process that aligns with existing good practices like privacy by design.

Key compliance takeaways include:

- the DIFC noted that systems with external commercial applications are likely to require certification, whereas purely internal, non-commercial systems processing employee data generally do not
- the DIFC certification is modelled on the Cross Border Privacy Rules ('CBPR') certification criteria; therefore, any AI system certified under this framework would meet the requirements of Regulation 10
- if an AI tool has obtained other recognised AI certifications, the Office of Data Protection would be open to considering those as well
- the DIFC is developing an AI assessment tool, which will align with the existing high risk processing ('HRP') assessment tool
- additional guidelines on Regulation 10 are expected to be published soon
- accredited certification bodies are expected to be in place by mid-2025
- the DIFC anticipates that relevant systems will be certified by around this time next year
- If only one component of a software system uses AI, certification is required solely for that component, not for the entire software
- regulation 10 also applies to AI tools located outside the DIFC if they are being used within the DIFC.

Feedback on the Automated Systems Officer ('ASO') role is being gathered via a survey. The enforcement of Regulation 10 will begin in January 2026.

The survey can be accessed [here](#). Regulation 10 can be found [here](#).

## 1.10 DIFC to Host FinTech Summit

The Dubai FinTech Summit 2025, hosted by the DIFC, will take place from 12 - 13 May 2025. This third edition of the summit will bring together global decision-makers, innovators, and investors to shape the future of finance.

The summit will be centered around innovation, inclusion, and impact, focusing on how technology, sustainability, and accessibility are transforming the financial landscape.

The key themes for 2025 are as follows:

- future of finance
- global economic trends
- blockchain and cryptocurrency
- financial innovation
- regulatory compliance
- investment outlook.

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

### 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 Online Registry for FATCA and CRS

On 7 April, the Financial Services Regulatory Authority ('FSRA') issued a reminder regarding the upcoming transition to the new Online Registry Solution for submitting the Foreign Account Tax Compliance Act ('FATCA') and Common Reporting Standard ('CRS') Entity Self-Certification Form ('SCF') for ADGM-domiciled entities.

The Online Registry replaces the previous email-based submission process. Registration and submission are mandatory for all ADGM-licensed entities, not just financial institutions. The SCF submissions must be completed via the ADGM Registration Authority Portal by 30 May 2025.

## 2.2 FSRA Issues Consultation Paper on Prudential Framework

On 9 April, the FSRA released Consultation Paper No. 2 of 2025 "Review of Prudential Framework for Lower Risk Firms". The paper sets out proposed amendments to the prudential framework for Authorised Persons classified as categories 3B, 3C, and 4 under the Prudential – Investment, Insurance Intermediation and Banking Rulebook ('PRU'), and invites feedback on the proposed changes.

Key proposals include:

- revisions to capital requirements for category 4 firms
- updates to reporting requirements for category 3B and 3C firms
- changes to professional indemnity insurance requirements under PRU.

You can read the Consultation Paper in full [here](#). Comments are welcome until 21 May 2025.

## 2.3 FSRA Issues Multiple Alerts

On 9 April, the FSRA issued an alert concerning misleading claims made by Trade World FX ('Trade FX'). The website purports to offer a platform for trading in FX currency pairs, commodities, stocks, indices, futures, bonds and cryptocurrencies and claims that Trade FX maintains a branch office in the ADGM.

The FSRA advises the public to note that:

- Trade FX has never been granted Financial Services Permission by the FSRA to conduct any regulated activities in or from ADGM
- is not incorporated in ADGM and has never been licensed to engage in any commercial activities within ADGM.

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

On 10 April, the FSRA issued an alert concerning the impersonation of Authorised Persons. The schemes include sophisticated scams and phishing attempts that misuse the name, logo, or branding of FSRA-licensed firms to deceive individuals into making payments or investing in fake financial products and opportunities. These fraudulent activities may appear through various channels, including fake websites, emails, letters, social media profiles, phone calls, group chats (such as WhatsApp or Telegram), text messages, and other forms of communication.

The FSRA urges all authorised firms to remain vigilant and raise awareness within their organisations about ongoing fraudulent schemes. Key points to be aware of:

- fraudsters may impersonate legitimate FSRA-licensed firms to create a false sense of trust and urgency



- communications may appear professional and originate from seemingly official sources, making them difficult to detect as fraudulent
- scammers often lure individuals with promises of non-existent investment opportunities or unrealistically high financial returns.

The FSRA advises all individuals and firms to take the following precautions to avoid falling victim to fraudulent schemes:

- always verify the identity of any person or organisation
- official communications from ADGM or FSRA-licensed firms will only come through verified channels
- never make payments or share personal information in response to unsolicited messages or unexpected requests.

Firms are encouraged to educate their teams and clients about these risks and to report any suspicious activity promptly.

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

On 30 April 2025, the FSRA issued a public alert regarding a scam involving a fake Telegram channel titled "Abu Dhabi Global Market." Telegram ("Telegram Messenger") is a cloud-based messaging platform that offers instant messaging and social media features across multiple devices. The scammers are promoting "investments" with "guaranteed investment returns," pressuring victims to transfer money into the scheme.

The fraudulent Telegram channel offers "investment packages" ranging from AED 1,000 to 15,000, with supposed returns of AED 15,000 to 700,000. The scammers further deceive victims by posting fake messages claiming to be from investors who have made substantial returns, thus convincing others to transfer money to specified bank accounts.

The FSRA highlights the following important points:

- ADGM does not operate a Telegram channel and does not directly contact individuals
- ADGM never offers investment opportunities or trading in financial products
- fraudsters may impersonate ADGM or FSRA to create a false sense of trust
- unsolicited communications from scammers may appear professional, making it harder to identify as fraudulent
- Scammers often promise unrealistic financial returns to lure victims

To protect yourself, the FSRA advises:

- verify the identity of anyone contacting you, as official communications from ADGM or FSRA-licensed firms will always come through verified channels
- avoid making payments or sharing personal information in response to unsolicited messages.

If in doubt, contact the FSRA directly using the contact information on the official website.

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

## 2.4 FSRA Issues Dear SEO Letter on Cybercrime Prevention

On 14 April, the FSRA issued Dear SEO Letter "Cybercrime Prevention – Avoiding Phishing Attacks". The letter seeks to raise awareness to authorised firms of the risks posed by phishing attacks.

To reduce the risk of phishing attacks and protect your organisation, the following key practices are recommended:

- establish awareness and training programs

- implement regular, organisation-wide cybersecurity training to help employees identify and respond to phishing threats
- recognise common red flags
  - educate staff to spot signs of phishing, such as generic greetings, suspicious email domains, urgent requests, unusual payment instructions, and poor grammar or design inconsistencies
- encourage internal reporting
  - promote a culture where employees feel comfortable reporting suspected phishing attempts
- review digital footprint
  - limit publicly shared sensitive information on websites and social media to reduce the chances of it being used in targeted phishing campaigns
- reinforce standard operating procedures
  - ensure employees follow and understand communication and transaction protocols, verifying unusual or high-risk requests through trusted channels
- implement two-factor authentication ('2FA')
  - strengthen account security by requiring a second form of verification alongside passwords
- adopt the principle of least privilege
  - grant employees only the access needed for their roles to minimise the impact of potential security breaches
- regularly back up data
  - perform frequent backups of critical data, store them securely offline, and routinely test recovery procedures to ensure quick restoration if needed.

By adopting these measures, authorised firms can significantly strengthen their resilience against phishing and other cybersecurity threats.

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

## 2.5 FSRA Issues Dear SEO Letter on Whistleblowing

On 17 April, the FSRA issued a Dear SEO Letter to authorised firms, reminding them of the upcoming implementation of the ADGM Whistleblower Protection Regulations 2024, which will come into effect on 31 May 2025.

All Authorised Persons and Recognised Bodies are required to establish arrangements that are appropriate to their nature, scale, and complexity by the deadline set by the FSRA. This includes implementing written policies and procedures for protected disclosures, facilitating such disclosures, and ensuring the maintenance of adequate records and information.

## 2.6 FSRA Publishes Business Plan

On 23 April, the FSRA published its business plan for 2025 - 2026, outlining the Regulatory Authority's vision and strategic direction for the next two years. The plan sets out key priorities aimed at further strengthening the FSRA's position as a progressive and globally recognised financial regulator, while supporting sustainable growth and fostering innovation within ADGM's dynamic financial ecosystem.

The business plan is centred around the following key strategic regulatory priorities:

- international regulatory alignment
  - continued collaboration with global standard-setting bodies to ensure regulatory coherence
- combatting financial crime
  - strengthened supervision, enforcement, and technology to fight money laundering, terrorist financing, and sanctions violations

- operational resilience
  - o enhanced frameworks to address cyber threats, geopolitical risks, supply chain issues, and fraud
- innovation
  - o advancement of Regulatory Technology ('RegTech') and Supervisory Technology ('SupTech') to support safe adoption of new financial technologies
- sustainable finance
  - o promotion of green and sustainability-linked financial products, and integration of climate risk management aligned with UAE's net-zero goals.

You can read the full business plan [here](#).

## 2.7 FSRA Supervision Outreach Session

On 30 April, the FSRA hosted a session providing key insights into its supervisory approach. The session covered an overview of the ADGM market, supervisory highlights and key outcomes from 2024, strategic priorities for 2025, and a forward-looking perspective on upcoming regulatory and supervisory developments.

Key highlights included a number of practical actions for consideration and preparation ahead of upcoming thematic reviews, risk assessments, and regulatory engagements:

- risk assessment and framework updates
  - o review and update the AML Business Risk Assessment ('BRA') to reflect the latest UAE National Risk Assessment ('NRA')
  - o conduct a gap analysis across all key areas: AML, cyber risk, outsourcing, operational resilience, and governance
- financial crime & AML/CFT compliance
  - o prepare for FSRA AML and financial crime thematic reviews and related questionnaires
  - o ensure suspicious transaction reporting ('STR') procedures are current and understood across the business
- cybersecurity and IT governance
  - o review and align cybersecurity policies and response plans with the new General Module ('GEN') Rulebook cyber requirements
  - o conduct a current-state cyber risk assessment, including third-party dependencies and vulnerabilities
  - o arrange cybersecurity and IT risk awareness training for staff, including executive management
- outsourcing and operational resilience
  - o assess all material outsourcing arrangements to ensure oversight, performance monitoring, and exit plans are in place
  - o review the business continuity plan ('BCP') and IT disaster recovery scenarios to ensure resilience during disruptions
  - o ensure board and senior management have active oversight of key outsourcing risks and dependencies
- governance and board engagement
  - o review governing body structure for adequacy of expertise, independence, and time commitment
  - o assess the quality and relevance of management information ('MI') provided to the board
  - o evaluate the effectiveness of board challenge, independence, and conflict of interest management
- conduct and business model
  - o validate the firm's business model documentation, conduct strategy, and product/service risk assessments
  - o ensure approved person records and fitness and propriety documentation are current and accessible

- review internal controls related to financial soundness, client money handling, and conflicts
- funds and digital assets
  - for fund managers, review proposed changes under the FSRA's funds strategic framework, including reporting and rulebook alignment with the International Organization of Securities Commissions ('IOSCO')
  - for firms in the digital asset space, validate AML/CFT measures and ensure compliance with VA-specific obligations including the travel rule
- training and awareness
  - roll out updated training sessions on AML/TFS, cyber incident handling, outsourcing oversight, and governance duties
  - conduct incident response exercises or scenario workshops for executive and operational teams.

## 2.8 FSRA Issues Consultation Paper on Cyber Risk

On 30 April, the FSRA released Consultation Paper No. 3 of 2025 "Proposed Enhancements to Cyber Risk Management". The proposed updates build upon the FSRA's 2020 Guidelines and the 2023 Discussion Paper on Information Technology Risk Management, aiming to establish consistent cyber risk expectations across all types of regulated entities.

Key proposals include revisions of the following rulebooks:

- General Rulebook ('GEN')
  - proposed a new section on Cyber Risk Management to be added to Chapter 3: Management, Systems and Controls
- Conduct of Business Rulebook ('COBS')
  - amendments to align conduct-related obligations (e.g. client protection and disclosures) with new cyber risk requirements
- Market Infrastructure Rulebook ('MIR')
  - amendments to bring Recognised Bodies into scope of the Cyber Risk Rules, alongside Authorised Persons
- Prudential – Insurance Business Rulebook ('PIN')
  - adjusted to reflect how insurers must incorporate cyber risk into their prudential and operational risk frameworks
- Captive Insurance Business Rulebook ('CIB')
  - updated similarly to PIN, with requirements tailored to captive insurers
- Prudential – Investment, Insurance Intermediation and Banking Rulebook ('PRU')
  - reflects how investment firms, banks, and intermediaries must account for cyber risks in capital adequacy and risk management
- Glossary Rulebook ('GLO')
  - definitions to be added or updated (e.g., "Cyber Risk," "Cyber Incident," "CRMF") to ensure consistent terminology across all rulebooks.

You can read the Consultation Paper in full [here](#). Comments are welcome until 11 June 2025.

### 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 Adopts New Enforcement Mechanism for AML/CFT Violations

On 5 April, the Capital Markets Authority ('CMA') of Kuwait has announced that it has taken a significant regulatory step by formalizing its enforcement mechanism for Anti-Money Laundering ('AML') and Combating the Financing of Terrorism ('CFT'). This move aligns with ongoing efforts to meet the FATF recommendations as part of Kuwait's ongoing mutual evaluation process.

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

#### 3.2 UAE Hosts First FATF Global Network Secretariats Roundtable

On 9 April, the General Secretariat of the National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organisations Committee ('GS-NAMLCFTC') hosted the Global Network Secretariats Retreat in Abu Dhabi, uniting top experts and decision-makers to strengthen global cooperation in the fight against money laundering/terrorist financing ('ML/TF'). The event brought together key regional bodies, including the Financial Action Task Force ('FATF') Secretariat, Asia/Pacific Group on Money Laundering ('APG'), Caribbean Financial Action Task Force ('CFATF'), the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism ('MONEYVAL'), Eurasian Group ('EAG'), Eastern and Southern Africa Anti-Money Laundering Group ('ESAAMLG'), Inter-Governmental Action Group against Money Laundering in West Africa ('GIABA'), Group of Latin American and Caribbean States against Money Laundering ('GAFILAT'), Middle East and North Africa Financial Action Task Force ('MENAFATF').

The forum fosters innovative solutions to enhance financial integrity and stability, underscoring the UAE's pivotal role in leading and coordinating regional and international efforts for impactful AMLCFT collaboration.

You can read the article [here](#).

#### 3.3 CBUAE Signs MoU

On 9 April, the Central Bank of the UAE ('CBUAE'), the National Bank of Kazakhstan, and the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market have signed a Memorandum of Understanding ('MoU') to strengthen cooperation and enhance information exchange in areas of mutual interest. The MoU outlines collaboration between the three parties on sharing information and expertise in financial market development, FinTech, and central bank digital currencies ('CBDCs'), including cross-border use. It also covers cooperation in Islamic finance, cybersecurity, supervisory practices, and technical support.

You can read the CBUAE article [here](#).

#### 3.4 UAE Completes National Risk Assessment on AML/CFT

On 17 April, the General Secretariat of the NAMLCFTC announced on its LinkedIn profile that the UAE has officially completed its National Risk Assessment on Anti-Money Laundering and Combating the Financing of Terrorism ('NRA AML/CFT'). This comprehensive assessment identifies key risks and outlines targeted actions to enhance the resilience of the UAE's financial system and ensure alignment with international standards. The UAE remains firmly committed to a secure and transparent financial future, working in close collaboration with global partners to combat financial crime. The NRA was officially published on 28 April.

The authorities request that all firms familiarize themselves with the updated NRA and take the following steps:

- review the updated UAE NRA report in its entirety

- identify, assess, understand, and mitigate ML and TF risks proportionate to the nature and size of each client's business
- conduct self-assessments and incorporate the findings into each client's AML/CFT policies and procedures
- ensure that AML/CFT manuals are regularly updated with effective and appropriate risk mitigation measures.

You can read the full NRA [here](#).

### **3.5 UAE Hosts Summit on the Role of DNFBPs in Combating Financial Crime**

On 16 – 17 April, the UAE hosted a high-level summit titled “The Role of the Designated Non-Financial Businesses and Professions (‘DNFBPs’) Sector in Combating Financial Crimes.” The event was organised by the Ministry of Economy in collaboration with the Executive Office for Control and Non-Proliferation (‘EOCN’).

A central focus of the summit was on enhancing customer due diligence and verification procedures, in line with targeted financial sanctions to prevent terrorism financing and the proliferation of arms. The event also aimed to empower the DNFBPs sector including real estate agents and dealers in precious metals to effectively implement the latest regulatory requirements.

You can read the EOCN announcement [here](#).

### **3.6 VARA Issues Consumer and Marketplace Alert**

On 23 April, the Dubai Virtual Assets Regulatory Authority (‘VARA’), in coordination with the Dubai Land Department (‘DLD’), has issued an official alert regarding entities that are falsely claiming or implying participation in the pilot phase of the DLD Real Estate Tokenisation Project (‘the Project’).

The Project was formally launched on 19 March 2025 as a limited pilot phase, involving a select group of participants approved jointly by DLD and VARA.

VARA and DLD urge stakeholders and members of the public to exercise due diligence and verify all claims of association with the Project through the official websites of VARA and DLD. This measure is in place to maintain the integrity of the pilot and protect market participants from potential misinformation.

Further details can be found [here](#).

### **3.7 SCA Issues Several Warnings**

In April, the Securities and Commodities Authority (‘SCA’) issued several warnings to investors regarding dealings with unlicensed companies, including Limited TRCFX Company, ANBCapitals, Empire Enigma Human Resources, Excellence FX Limited, and an unknown party operating the website "dubaifinancial.org". These entities are not authorised to carry out any financial activities or services regulated by the SCA.

The SCA has informed the public that it assumes no responsibility for any transactions conducted with these companies and strongly urges investors to verify the legitimacy of any entity before entering into agreements or making financial transfers.

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

#### Further information

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

## 4. INTERNATIONAL UPDATES

### 4.1 FATF Updates Consolidated Ratings

On 23 April, the FATF published an updated consolidated ratings table. The table summarises jurisdictions' progress against the 40 FATF recommendations. The recommendations assess the jurisdiction's maturity against AML, counter terrorist financing ('CTF') and proliferation financing measures.

You can read the consolidated rating table [here](#).

#### Further information

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



## 5. ENFORCEMENT ACTIONS

### 5.1 FSRA Imposes Fines

On 14 April, the FSRA announced that it took enforcement action following an investigation into serious regulatory breaches and misconduct involving the Hayvn Group of Companies (operating as 'HAYVN'), its former CEO Christopher Flinos, and related entities.

The investigation uncovered significant misconduct in the operations of three related party companies and Mr. Flinos. The FSRA acted to ensure that no ADGM client assets or funds were lost as a result of the breaches. A total of US\$ 8.85M in fines has been imposed.

A summary of the contraventions are as follows:

- unlicensed activities
  - Hayvn Cayman and AC Holding conducted significant unlicensed financial services activity related to virtual assets in ADGM from 2018 to 2024, including unauthorised payments and arranging services
- misuse of client funds
  - Hayvn ADGM exceeded the scope of its financial services permission by routing client transactions through AC Holding's unregulated accounts without proper safeguards
- AML failures
  - Hayvn ADGM failed to maintain adequate systems and controls, including those required under FSRA's Anti-Money Laundering rules, and did not properly recognise or record all client relationships
- misleading information and documents
  - over 200 false and misleading documents were created and submitted to banks to support AC Holding's operations, under the direction of Christopher Flinos and with the involvement of Hayvn Cayman and AC Holding
- deception of the regulator
  - all three entities, along with Flinos, provided false and misleading information to the FSRA during its investigation, undermining the integrity of the regulatory process
- leadership accountability
  - as SEO and CEO, Christopher Flinos was found to have played a central role in the misconduct and failed to act with integrity or ensure compliance with ADGM regulations.

You can read the FSRA article [here](#).

### 5.2 ADGM RA Imposes Fines

On 14 April, the ADGM Registration Authority ('RA') announced that it imposed fines of US\$ 3.6M on Special Purpose Vehicle AC Holding and Christopher Flinos and banned him as a director of any ADGM-based company for 15 years.

The RA's investigation revealed that AC Holding exceeded the scope of its ADGM SPV license by acting as an investment company and providing unauthorized financial services, including processing cryptocurrency-to-fiat transactions. Additionally, it submitted false annual accounts to the Registration Authority for the years 2019 to 2022.

The RA found that Christopher Flinos engaged in fraudulent trading by using AC Holding to facilitate unlicensed cryptocurrency conversion transactions, misleading multiple parties about the nature of these activities. He also

played a key role in falsifying and submitting hundreds of company documents to fraudulently maintain bank accounts.

You can read the FSRA article [here](#).

### 5.3 CBUAE Imposes Financial Sanction on Bank

On 21 April, the CBUAE has imposed a financial sanction on a UAE-based bank for failing to comply with anti-money laundering and counter-terrorism financing regulations. The penalty follows an assessment by the CBUAE, which found deficiencies in the bank's policies and procedures. The CBUAE continues to enforce compliance to uphold the transparency and integrity of the UAE's banking and financial system.

You can read the notice [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](mailto: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 2, Gate Village Building 7,  
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.