Date: 29 January 2026

Notice No: FSRA/FCCP/22/2026

To: Senior Executive Officers (SEO) and Principal Representatives (PR) of FSRA's Authorised Persons.

Dear SEO/PR,

RE: Updates to Information Technology ("IT") and Cyber Incident Reporting

This notice informs Authorised Persons of revisions to the IT & Cyber Incident Reporting Templates and reiterates applicable reporting obligations.

These changes follow the public consultation on the Cyber Risk Management (CRM) Rules. It also aligns with the Financial Stability Board (FSB) April 2025 update and the FSRA's adopted incremental reporting approach. The CRM Rules under GEN 3.5 come into effect on 31 January 2026.

Summary of the updates

- **Initial reporting template:** streamlined to capture essential information required for an initial risk assessment and revised to reflect consultation feedback.
- **Progressive reporting template:** enhanced to support timely and accurate ongoing updates as incidents are being contained and investigated.
- **Reporting timeline**: GEN 8.10 continues to require immediate notification upon discovery of an incident. The CRM Rules (GEN 3.5.18) introduce a 24-hour backstop for initial reporting. Authorised Persons must notify the FSRA immediately upon discovery of a suspected material cyber incident and, in any event, no later than 24-hours after they become aware of information that reasonably suggests such an incident has occurred.

Notification mechanism

- **Initial report:** Authorised Persons are required to complete the updated IT & Cyber Incident Initial Report – Template A, email it to incidents.fsra@adgm.com and ensure to copy their FSRA lead supervisor or pooled supervision team on the submission.
- **Progressive updates:** Authorised Persons are required to submit subsequent updates using the updated IT & Cyber Incident Progressive Report - Template B to the same mailbox. Each submission should reflect the most current and accurate information available. The FSRA supervisor will determine the required update frequency on a case-by-case basis, depending on incident severity and complexity.

Access to templates

The updated incident reporting templates (Template A — Initial Report; Template B — Progressive Report) are available on the following ADGM webpages:

- *Financial and Cyber Crime Prevention Forms*
- *IT Risk Management*

Authorised Persons are required to use these templates for all relevant IT & Cyber incident submissions going forward.

Other reporting obligations

Authorised Persons are also reminded of reporting obligations to other regulatory bodies where applicable (e.g., data protection breach, the FIU for suspicious activity/transaction report) and law enforcement where appropriate.

Contact

For any further clarifications, Authorised Persons are required to reach out by email to fccp-cybercrimeprevention@adgm.com.

Your continued cooperation and vigilance are crucial to maintaining the integrity, security, and stability of the ADGM's and UAE's financial systems.

Sincerely,

Financial & Cyber Crime Prevention