Date: 22 January 2026

Notice No: FSRA/FCCP/15/2026

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

Dear SEO / PR,

RE: Cyber Risk Survey Findings and Recommendations

The Financial and Cybercrime Prevention department ("FCCP") of the Financial Services Regulatory Authority ("FSRA") conducted a survey in Q3 2025 to better understand how Authorised Persons are managing cyber risk. The survey was sent to 315 firms and achieved an 83% response rate (263 respondents).

The survey findings provide a valuable insight into the current state of governance, technical controls and cyber resilience across FSRA regulated entities.

The growing reliance on technology within the financial sector has increased financial institutions' exposure to digital vulnerabilities that can be exploited by cybercriminals. To mitigate these risks, Authorised Persons & Recognised Bodies (hereinafter referred to as 'Firms') are required to establish a comprehensive cyber risk management framework and maintain effective and robust systems and controls to address cybercrime risk.

This notice provides Firms with an overview of identified cyber risks and outlines the actions expected to mitigate them.

It is issued to raise awareness and support ongoing compliance. It does not set out all the obligations of Firms in relation to cyber risk management. Firms should always refer to relevant rules and guidance to ensure full compliance.

Overview

The survey questions specific to cyber risk management (*attached as Annex A*) are closely aligned with the Cyber Risk Management Rules, which take effect on the 31st of January 2026. Under these rules, Firms are required to integrate cyber risk management into their existing operational risk frameworks, building on the FSRA's Information Technology Risk Management Guidance and Governance Principles and Practices to Mitigate Cyber Threats and Crime.

Accordingly, the recommendations outlined in this notice set out the FSRA's expectations in relation to the key compliance areas assessed in the survey, namely:

- Cyber Risk Management Framework & Governance
- Identification and Assessment of Cyber Risk
- Protection of Information Technology (IT) Assets against Cyber Incidents
- Monitoring and Testing
- Detection, Response and Recovery

Key Takeaways and Recommendations

1. Cyber Risk Management Framework & Governance

This area was assessed through four separate questions covering board representation, policies, management forums and defined operational roles.

Key Takeaways	Recommendations
• Cyber risk continues to be a core business risk and warrants ongoing board-level attention. • A lack of clearly defined roles and responsibilities for operational cyber risk management can create ambiguity in accountability, particularly ineffective risk management during cyber incidents.	• Firms must ensure the framework is documented and approved by the board. • Firms need to establish clear board-level representation and responsibility for cyber risk and ensure management forums are in place to support decision-making. This should include identifying which risks to avoid, accept or mitigate. • Firms are expected to assign clear operational roles for cyber risk management to ensure effective oversight, accountability and timely response during incidents. The board/senior management must hold ultimate responsibility for cyber risk and ensure it is managed effectively.

2. Identification and Assessment of Cyber Risk

This area was assessed through four separate questions covering cyber risk assessments, IT asset classification, vulnerability management practices and third-party cyber risk management.

Key Takeaways	Recommendations
• IT asset classification and vulnerability management practices work in tandem. Effective identification and assessment of cyber risk rely heavily on accurate IT asset classification and structured vulnerability management processes. • Unidentified assets and unpatched vulnerabilities are among the more commonly reported attack vectors exploited by cyber criminals targeting financial institutions. • Firms lacking comprehensive asset inventories and systematic vulnerability management cannot adequately prioritize security resources or ensure appropriate protection of critical systems, resulting in heightened risk exposure. • The increasing reliance on third-party providers introduces additional cyber risk vectors, particularly when cyber risk expectations and reporting obligations are not formally embedded in outsourcing arrangements.	• Firms are expected to identify all ICT assets and maintain an up-to-date inventory, including classification of assets by criticality and sensitivity to ensure vulnerabilities are promptly addressed. • Service provider agreements should include explicit cyber incident reporting requirements, as well as clearly defined cyber security standards. Firms should enhance ongoing oversight to ensure continued compliance with these expectations.

3. Protection of ICT Assets against Cyber Incidents

This area was assessed through three separate questions. Namely, security awareness and training, Cyber Threat Intelligence (CTI) sources and technical security controls.

Key Takeaways	Recommendations
• Firms without a formal risk assessment may be operating with significant blind spots in their security posture. • Employees often constitute the first line of defence against social engineering attacks. • Effective security awareness training is not merely a compliance exercise but a critical component of operational resilience. Regular, comprehensive and engaging programmes strengthen an organisation's security posture by addressing the human element of cyber risk. • Basic cyber security practices and controls (passwords, multi-factor authentication, anti-malware solutions) are widely adopted, while more advanced or resource-intensive controls show lower uptake. This is expected, as such advanced measures should remain commensurate to the nature, scale and complexity of a firm's operations.	• Firms should establish minimum standards for cyber security awareness training programmes, focusing on frequency, the content delivered and its effectiveness. This includes how to respond effectively when incidents occur or suspicions arise. • Firms should participate in threat-intelligence sharing communities and ensure CTI is integrated into internal processes to strengthen overall cyber resilience. • Firms are expected to implement appropriate encryption techniques to protect the confidentiality and integrity of sensitive data both at rest and in transit. • Firms should be implementing strong identity and access management controls and adopt the principle of least privilege to reduce the firm's attack surface area.

4. Monitoring and Testing

This area was assessed through two questions relating to logging and monitoring and adversarial testing.

Key Takeaways	Recommendations
• The limited adoption of advanced testing methodologies, such as penetration testing and red teaming, reduces firms' ability to identify sophisticated or emerging vulnerabilities and may leave critical gaps undetected.	• Larger and more complex organisations should implement advanced testing methods that simulate real-world attack scenarios. These practices can help uncover previously unknown vulnerabilities.

5. Detection, Response and Recovery

This area was assessed through two separate questions. Namely, cyber incident management approaches and monitoring controls.

Key Takeaways	Recommendations
• A formal cyber incident response plan is essential to ensure timely detection, containment and recovery from cyber incidents, thereby minimising operational disruption and wider business impact. • Firms that have incident management processes in place but do not test them regularly may find their response capabilities less effective during real-time incidents.	• Firms should establish and maintain formal incident response plans, supported by regular testing, simulations and post-incident reviews to improve on security posture and strengthen overall response readiness and resilience over time.

The institutionalization of a robust cybercrime prevention framework is a key priority for the FSRA and is central to our regulatory efforts to safeguard the integrity of the financial services industry in the ADGM. It also forms part of the broader UAE national efforts to combat cybercrime.

The FSRA will continue to monitor global industry best practice in relation to cyber risk management to ensure that effective control standards are maintained by Firms.

For any further clarification, Firms are required to reach out by email to FCCP-CybercrimePrevention@adgm.com.

Sincerely,

Financial & Cyber Crime Prevention

Appendix A: Cyber Risk Management Survey Questions[1]

Ref. Notice No: FCCP/FCCP/15/2026 - *RE: Cyber Risk Management Survey Findings and Recommendations*

1. Does the firm have representation on the board for Cyber Risk matters?
   Yes/No

2. Does the firm have management forums/committees that review decisions relating to Cyber risk management?

   If yes, describe the responsibilities of such forums/committees, frequency of meetings and the technology related metrics reported to such forums/committees.

3. Does the firm have policies, procedures, and/or manuals to govern cyber risk management
   Yes/No

4. Does the firm have defined roles and responsibilities for individuals involved in operational cyber risk management.
   Yes/No

5. Have cyber risks relating to the firm and its business activities been formally identified and impact assessed?
   Yes/No

6. a) Does the firm have a due diligence process to ensure that third-party providers meet cybersecurity requirements?
   b) Does the firm include cybersecurity requirements in agreements with third-party service providers?
   c) Does the firm include cyber incident reporting requirements in agreements with third party service providers?
   d) Are checks conducted to review ongoing compliance with the firm's cybersecurity requirements?

   i. Yes/No
   ii. Yes/No
   iii. Yes/No
   iv. Yes/No

7. Which of the following sources or services does the firm use for cyber threat intelligence?

   (Select all that apply and specify vendor name if applicable)

   a) In-house resources or open-source intelligence analysts
   b) Managed Service Provider / Third-party vendor
   c) FS-ISAC (Financial Services Information Sharing and Analysis Centre)
   d) Alerts from the Cyber Security Council
   e) None of the above

[1] Extract from the AI and Cyber Risk Survey communicated to firms in the FSRA Outsourcing Thematic Review and accompanying surveys notice issued 09th June 2025.

8. Does the firm have established processes and channels to distribute threat intelligence to appropriate groups within the organisation, such as risk management and front-line IT security staff members?
   Yes/No - If yes, please describe.

9. Does the firm identify and classify IT assets (Hardware and Software) based on their criticality and sensitivity?

   Yes/No

10. Does the firm have a vulnerability management process? (An approach to identifying, assessing, remediating and mitigating vulnerabilities in an organisations IT system, networks, applications and devices?

    Yes/No

11. Please confirm if the firm has the following controls implemented: *(Select all that apply)*

   a) Password practices
   b) Multi-Factor Authentication (MFA) practices
   c) Anti-malware software installed on workstations
   d) Anti-malware software installed on servers
   e) Firewall at Firm's network perimeter to restrict unauthorised access
   f) Intrusion prevention / detection system
   g) Data encryption (Removeable media/hard drives)
   h) Encryption of sensitive data in transit?
   i) Regular data back-up processes?

12. Does the firm conduct training for all employees on technology risk management / cybersecurity and cybercrime awareness / data protection practices?

    Yes/No - If yes, describe the scope of the training and frequency.

13. Does the firm have a process of logging and monitoring to detect and investigate incidents?

    Yes/No

14. Which of the following best describes the firm's approach to IT & cyber incident management?
    a) The firm has an approved incident management plan with 24/7 coverage, conducts regular exercises and includes a post incident review.
    b) The firm has an approved incident management plan and conducts regular exercises.
    c) The firm has an approved incident management plan but does not conduct regular exercises.
    d) The firm has an informal process to manage incidents.
    e) The firm does not have an incident management process.

15. What methods of adversarial testing does the firm employ? (*Select all that apply*)
    a) Penetration testing;
    b) Red teaming;
    c) Bug bounty programs;
    d) Social engineering exercises;
    e) None