FSRA IT Risk Management Expectations: A High-Level Summary

April 2, 2025

The Financial Services Regulatory Authority ('FSRA') IT Risk Management Guidance, published in November 2024, provides a structured approach to help firms in the Abu Dhabi Global Market ('ADGM') manage information technology ('IT') related risks, ensuring resilience against cyber threats.

The guidance is aligned with global best practices and regulatory standards, reflecting the increasing reliance on technology within financial services and the growing risks from cyber threats.

Key Sections of the Guidance:

1. Establishing a Culture of Effective IT Risk Management: This section emphasises governance, risk management frameworks, incident management, and the oversight of third-party service providers.
2. Managing an IT Environment: Focuses on asset management, system lifecycles, IT infrastructure, resilience, and incident response protocols.
3. Interacting Securely: Addresses access controls, secure transactions, and cryptography.
4. Leveraging Emerging Technologies: Covers governance and risk management related to emerging technologies, such as artificial intelligence ('AI') and decentralised platforms.

FSRA's Key Expectations for Regulated Firms

The FSRA expects regulated entities in ADGM to adopt IT risk management practices proportionate to their size, complexity, and business activities. Core expectations include establishing strong IT governance, conducting regular risk assessments, and implementing robust cybersecurity controls.

Core Areas of Focus:

- **Governance:** Senior management must ensure that the IT strategy aligns with business goals, while establishing accountability and competence in IT risk management.
- **Risk Management:** Firms are required to implement a comprehensive risk management framework, including incident management and mechanisms for addressing problems.
- **Third-Party Risk Management:** Firms must oversee third-party providers, ensuring that service level agreements ('SLA') address cybersecurity risks and operational disruptions.
- **Cybersecurity Resilience:** Firms must demonstrate the ability to withstand and recover from cyber incidents, with clear incident response protocols and continuity planning.
- **Secure Digital Interactions:** Firms must protect customer transactions with strong access controls, encryption, and fraud mitigation measures.

Tips for Firms to Strengthen IT Risk Management

1. Establish a Robust Governance Structure:

- Ensure that senior executives and compliance officers are actively involved in overseeing IT risks, ensuring alignment with business objectives, and holding themselves accountable for managing these risks. It is not just an IT department obligation!

2. Implement Regular Risk Assessments:

- Conduct periodic IT risk assessments to identify vulnerabilities and address potential threats. These assessments should be part of a broader, ongoing risk management framework.

3. Enhance Cybersecurity Measures:

- Regularly test your incident response and recovery plans. Cultivate a cybersecurity-aware culture within the organisation by ensuring that all employees are trained to recognise and respond to cyber threats.

4. Strengthen Third-Party Vendor Management:

- Implement clear protocols for assessing and monitoring the cybersecurity posture of third-party providers. Ensure that SLAs include provisions for managing cyber risk and disruptions.

5. Leverage Emerging Technologies Safely:

- When adopting advanced technologies like AI or decentralised platforms, ensure that their development, use, and deployment align with established governance and security frameworks.

Recent IT and Cyber Issues in the UAE and Worldwide

Recent cyber threats have highlighted the urgent need for stronger cybersecurity across both the UAE and the world. In the UAE, the “State of the UAE – Cybersecurity Report 2024” reveals an uptick in cyberattacks targeting financial institutions and critical infrastructure. Notably, a significant cyberattack in 2023 disrupted the UAE’s financial sector, underscoring vulnerabilities in existing systems. This has spurred the UAE government to enhance regulations, which mandates stricter resilience measures for key sectors like finance.

On the global stage, incidents such as the 2023 MOVEit Data Breach and the 2021 Colonial Pipeline ransomware attack have further highlighted the critical need for robust cybersecurity in industries like data storage and energy infrastructure. These events collectively point to the growing necessity of advanced cybersecurity strategies to protect essential systems and sensitive data.

Sources: *State of the UAE – Cybersecurity Report 2024, Bleeping Computer, CISA.*

Actions for Firms to Implement

Action	Description
Governance Framework	Establish a clear IT governance structure, ensuring senior management's accountability and regular reporting on IT risks.
IT Risk Assessment	Establish a clear IT governance structure, ensuring senior management's accountability and regular reporting on IT risks.
Incident Response & Continuity Planning	Develop and regularly test incident response plans, ensuring business continuity during IT disruptions or cyber incidents.
Employee Awareness & Training	Conduct mandatory cybersecurity awareness training for all employees, including topics on phishing, secure access, and incident reporting.
Third-Party Vendor Risk Management	Implement a vendor risk management framework, including vetting third-party providers and continuous monitoring of their cybersecurity practices.
System Lifecycle Management	Establish a clear process for managing IT systems throughout their lifecycle, including acquisition, development, testing, and decommissioning.
Access Controls & Encryption	Implement strong access controls (e.g., multi-factor authentication) and cryptographic measures to protect sensitive data and transactions.
Cyber Resilience Testing	Conduct regular cyber resilience tests, including simulated cyberattacks, to assess your organisation's readiness to respond and recover.
Emerging Technologies Oversight	If using AI or decentralised technologies, ensure proper governance, security, and monitoring protocols are in place.

What Next?

As technology evolves and becomes more integrated into financial services, firms must prioritise strengthening their IT risk management frameworks to protect against cyber threats and operational disruptions. By implementing the FSRA IT Risk Management Guidance, adopting cybersecurity best practices, and remaining vigilant against emerging risks, firms can comply with regulatory requirements and position themselves as leaders in risk management and resilience.

The Waystone Cybersecurity Team is well-equipped to assist organisations in navigating the complexities of these regulations, implementing effective cybersecurity frameworks, and staying ahead of both global and regional cyber threats. Contact us today to learn how we can support your firm in building a robust and compliant IT risk management strategy.

Contact us →