Cyber Risk Management Enhancement at ADGM: Key Insights and Compliance guidance for firms

BDO UAE | Advisory Services | 2025

Introduction

In today's rapidly evolving digital landscape, cyber threats have become increasingly sophisticated and widespread, posing significant risks to financial institutions and their stakeholders. Recognizing these challenges, the Abu Dhabi Global Market's (ADGM) Financial Services Regulatory Authority (FSRA) has updated its risk management framework to incorporate enhanced requirements for managing cyber risks. These updates are aimed at strengthening the cyber resilience of firms operating within ADGM by ensuring that their overall risk management practices are aligned with global best practices and the UAE's national cybersecurity strategy.

The updated framework mandates a comprehensive integration of cyber risk management into firms' overall risk governance, with particular emphasis on robust controls, proactive risk assessments, and effective incident response mechanisms. Furthermore, there is heightened scrutiny on third-party vendor and IT service provider risks, reflecting the growing dependence on external technology providers in today's financial ecosystem.

With the new regulations coming into effect on 31 January 2026, it is imperative that firms understand the scope of these changes and take timely action to ensure compliance. This entails not only technical upgrades and policy revisions but also enhanced governance and employee training to foster a culture of cyber resilience. Failure to comply may result in significant penalties, reputational damage, and operational disruptions.

This presentation outlines the key changes introduced by the FSRA, discusses their implications for firms, and provides actionable guidance on how to meet these new requirements efficiently. It also highlights the comprehensive support services that BDO UAE offers to help firms navigate these enhancements and achieve full compliance within the stipulated timeline.

What's changing?

- **Mandatory Cyber Risk Integration :**
  All firms operating in ADGM must have a board-approved Cyber Risk Management Framework (CRMF) fully integrated into their broader risk management. This ensures cyber risk is addressed strategically and overseen at the highest level, making cybersecurity a core part of business risk management rather than a siloed IT issue.

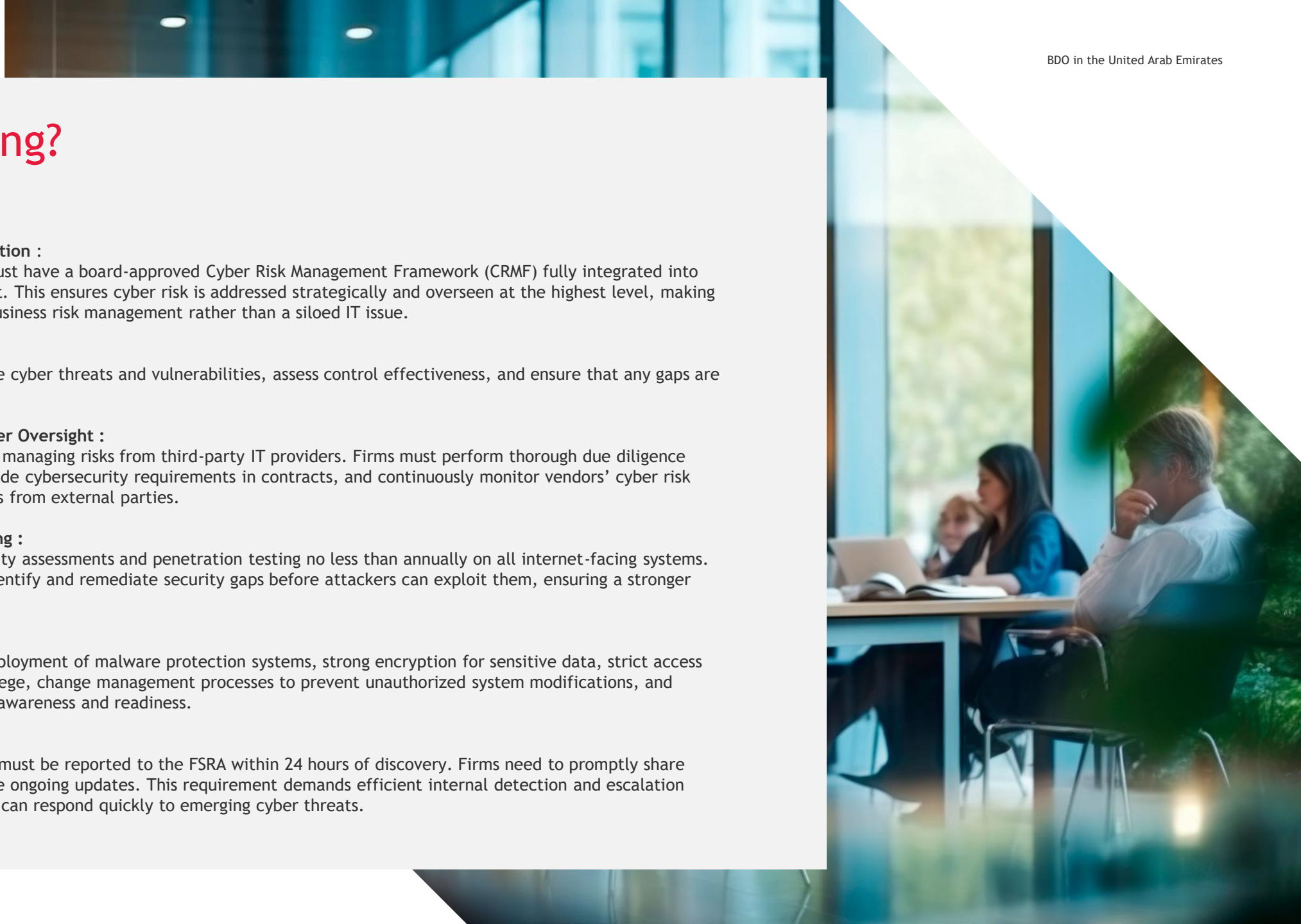
- **Expanded Scope :**
  Regularly identify and evaluate cyber threats and vulnerabilities, assess control effectiveness, and ensure that any gaps are addressed.

- **Vendor and IT Service Provider Oversight :**
  There is an increased focus on managing risks from third-party IT providers. Firms must perform thorough due diligence before engaging vendors, include cybersecurity requirements in contracts, and continuously monitor vendors' cyber risk posture to avoid vulnerabilities from external parties.

- **Regular Testing and Monitoring :**
  Firms must conduct vulnerability assessments and penetration testing no less than annually on all internet-facing systems. This proactive testing helps identify and remediate security gaps before attackers can exploit them, ensuring a stronger defense posture.

- **Technical Safeguards :**
  Mandatory controls include deployment of malware protection systems, strong encryption for sensitive data, strict access controls to enforce least privilege, change management processes to prevent unauthorized system modifications, and ongoing staff training to raise awareness and readiness.

- **Rapid Incident Reporting :**
  Any significant cyber incident must be reported to the FSRA within 24 hours of discovery. Firms need to promptly share preliminary details and provide ongoing updates. This requirement demands efficient internal detection and escalation processes, ensuring regulators can respond quickly to emerging cyber threats.



Why this matters

These changes will strengthen the financial sector's operational resilience, protect clients and markets, and align ADGM with the UAE's national cybersecurity strategy and international best practices. Post-implementation, FSRA will conduct supervisory reviews and may require annual cyber risk management returns depending on compliance levels.

Compliance Timeline

- Transition Period: 6 months to prepare for compliance.
- Compliance Deadline: Full compliance required by 31 January 2026.

Penalties & Implications

FSRA may impose penalties such as fines, increased supervisory scrutiny, or operational restrictions for non-compliance. Firms are encouraged to engage proactively with FSRA regarding any uncertainties.

What should your business do?

- **Develop or update your Cyber Risk Management Framework**:
  Create or revise a board-approved framework that integrates cyber risk into overall firm governance and aligns with FSRA requirements.
- **Perform cyber risk assessment**:
  Regularly identify and evaluate cyber threats and vulnerabilities, assess control effectiveness, and ensure that any gaps are addressed.
- **Enhance due diligence and oversight of third-party ICT providers:**
  Assess vendors' cybersecurity capabilities before onboarding, include security terms in contracts, and monitor their ongoing risk posture.
- **Schedule and conduct regular vulnerability scans, red-team exercises, and penetration tests:**
  Perform at least annual scans and tests on internet-facing systems to detect and fix security weaknesses promptly.
- **Implement technical controls including malware defense, encryption, and access policies:**
  Use strong malware protection, encrypt sensitive data, enforce strict access controls, and manage changes securely.
- **Prepare for prompt 24-hour cyber incident reporting via FSRA's established channels:**
  Set up efficient detection and reporting processes to notify FSRA within 24 hours of a material cyber incident.
- **Train staff across departments on cyber risk policies and incident response:**
  Provide regular cyber awareness and response training to all relevant employees to strengthen organizational resilience.
- **Review contracts and operational policies with third-party technology suppliers:**
  Ensure contracts include clear cybersecurity requirements and update policies to reflect enhanced third-party risk oversight

How BDO can support you?

BDO offers tailored services to assist firms in achieving compliance, including risk assessments, framework development, vendor oversight, technical testing coordination, incident reporting preparation, training programs, and ongoing regulatory liaison. our services include:

- **Framework Development and Enhancement**
  BDO helps develop or update your Board-approved Cyber Risk Management Framework (CRMF), translating regulatory requirements into actionable policies, controls, and incident response plans suited to your firm's complexity.
- **Comprehensive Cyber Risk Impact Assessment**
  We assess your current cyber risk management against FSRA requirements, pinpoint strengths and gaps, and provide a prioritized remediation roadmap tailored to your firm's risk profile.
- **Technical Controls & Testing Support**
  We coordinate vulnerability assessments, penetration testing, and red-team exercises; assist in remediation planning; and advise on key technical controls including encryption, malware defense, access management, change control, and patching.
- **Vendor and Third-Party Risk Oversight**
  We support establishing or enhancing third-party cyber risk programs through due diligence, risk scoring, contract reviews, monitoring, and compliance documentation to reduce supply chain risks.
- **Cyber Incident Reporting Preparation**
  BDO guides firms on FSRA's incident reporting requirements, develops and tests detection and reporting workflows, assists with timely notifications, and runs simulation exercises to ensure preparedness.
- **Training and Awareness Programs**
  We deliver tailored workshops and e-learning modules for all levels—from boards to operational staff—covering cyber risk awareness, regulatory reporting duties, and incident response to build cyber resilience.
- **Regulatory Liaison and Ongoing Support**
  Acting as your FSRA liaison, BDO handles queries, clarifies guidance, manages submissions, keeps you updated on regulatory changes, and provides ongoing advisory support beyond compliance.

Shivendra Jha
Partner & Head of Advisory Services

shivendra.jha@bdo.ae
+971 55 572 0269

Madan Mohan
Director - Technology Advisory Services

madan.mohan@bdo.ae
+971 55 224 6250