limitless consulting

FSRA Cyber Risk Survey

Summary of Findings and Recommendations By Limitless Consulting

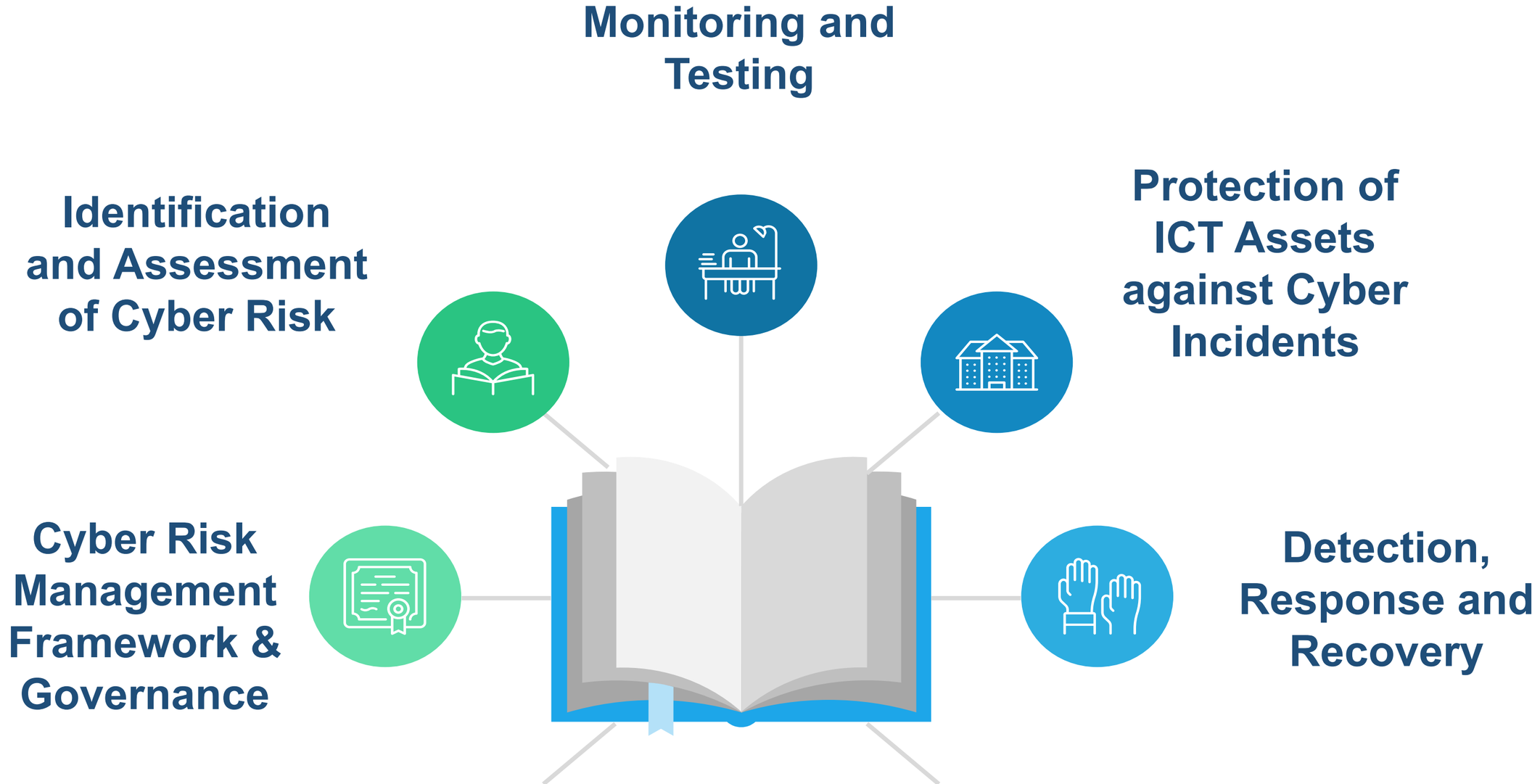
April 2026

Unlock your way to limitless potential

Cyber Risk Survey Results

Summary of Key Findings

FSRA carried out a Cyber Risk Review in Q3 of 2025 and issued findings summary via a notification. This document is aimed to present a summary of the results in relation to the observed gaps and supervisory expectations to strengthen cyber resilience. Below diagram indicates the key areas that were focused as part of this review:



Action Required

Financial Services Regulatory Authority (FSRA) underscores the importance of a comprehensive and proactive approach to cybercrime prevention in safeguarding the stability and integrity of Abu Dhabi Global Market's (ADGM) financial sector.

Firms are expected to embed cyber risk management within their overall governance and risk frameworks, ensuring strong board oversight, clearly defined accountability, and continuous improvement of technical and organisational controls.

Cyber Risk Survey Results

Key Takeaways and Recommendations

Area	Key Takeaways	Recommendations
Cyber Risk Management Framework & Governance	- Cyber risk is a core business risk requiring board-level attention. - Undefined roles and responsibilities can create ambiguity and reduce effectiveness during incidents.	- Document and obtain board approval of the cyber risk framework. - Ensure clear board-level representation and decision-making forums. - Assign defined operational roles, board/senior management holds ultimate accountability.
Monitoring and Testing	- Limited use of advanced testing (penetration/red teaming) reduces ability to detect sophisticated vulnerabilities.	- Implement advanced testing for larger/complex organisations to simulate real-world attacks and identify hidden vulnerabilities.
Detection, Response and Recovery	- Formal incident response plans are essential to minimise operational disruption. - Untested processes reduce effectiveness during real incidents.	- Develop and regularly test cyber incident response plans to ensure timely detection, containment, and recovery.
Identification and Assessment of Cyber Risk	- Effective cyber risk assessment relies on accurate IT asset classification and vulnerability management. - Unpatched vulnerabilities and unidentified assets are common attack vectors. - Third-party providers introduce additional risks if expectations are unclear.	- Maintain an up-to-date inventory of all Information and Communication Technology (ICT) assets, classified by criticality and sensitivity. - Include cyber risk expectations and incident reporting obligations in service provider agreements. - Ensure ongoing oversight of third-party compliance.
Protection of ICT Assets against Cyber Incidents	- Lack of formal risk assessment creates blind spots. - Employees are the first line of defence; awareness is critical. - Basic technical controls widely adopted; advanced controls less so.	- Implement structured, regular security awareness training covering incident response. - Participate in threat intelligence sharing and integrate Cyber Threat Intelligence into internal processes. - Apply strong encryption, identity, and access management, adopt least privilege principle. -