waystone | Compliance Solutions

DFSA High-Level Cyber Risk Management Guide

April 2, 2025

In line with the Dubai Financial Services Authority ('DFSA') regulations, specifically General Rulebook ('GEN') Rule 5.5 on Cyber Risk Management, DFSA-authorised firms should have already taken steps to establish frameworks to identify, assess, and mitigate cyber risks.

The DFSA has emphasized the need for firms to adopt strategies that protect their Information and Communication Technology (ICT) assets and ensure resilience against cyber threats. As firms work to meet these requirements, the implementation of a Cyber Risk Management Framework ('CRMF') is essential to maintaining robust security practices.

This guide highlights key areas for improving cybersecurity practices and offers actionable tips that firms can apply to strengthen their security posture.

1. Cyber Risk Management Framework

A CRMF is essential for identifying and mitigating cyber risks. It should be integrated into a firm's business strategy and daily activities.

Real-Life Example: A financial institution regularly reviews its ICT assets, classifying them based on their sensitivity to ensure mission-critical systems are protected by more stringent security measures.

Tip for Firms:

— Regular Cyber Risk Assessment: Continuously evaluate internal vulnerabilities and external threats to adapt to an evolving cyber risk landscape.

2. Governance and Responsibility

Clear ownership of cybersecurity responsibilities ensures that security practices are implemented, monitored, and maintained effectively.

Real-Life Example: A global tech company appoints a Chief Information Security Officer ('CISO') to oversee all cybersecurity activities, reporting directly to the board.

Tip for Firms:

— Appoint a Cybersecurity Officer: Designate a CISO or equivalent to manage cybersecurity strategy and execution.

3. Third-Party Risk Management

Managing cybersecurity risks from third-party vendors is crucial for businesses relying on external service providers.

Real-Life Example: After a cloud storage provider breach, a company strengthens its vendor assessment processes to ensure security standards are met.

Tip for Firms:

— Third-Party Due Diligence: Conduct thorough assessments of third-party vendors to ensure they meet your firm's cybersecurity standards.

4. Protecting ICT Assets

Implementing technical controls such as firewalls, anti-malware software, and encryption is fundamental to protecting ICT assets.

Real-Life Example: A financial firm uses anti-malware software to scan incoming emails, preventing malware infections from spreading.

Tip for Firms:

— Multi-layered Security: Implement a combination of firewalls, anti-malware tools, and encryption for comprehensive protection.

5. Change Management

Managing updates, patches, or changes to IT systems is critical for addressing potential security risks.

Real-Life Example: A company tests new enterprise software in a controlled environment to identify and mitigate security vulnerabilities.

Tip for Firms:

— Testing New Software: Ensure thorough testing in a development environment to detect vulnerabilities before deployment.

6. Security Awareness and Training

Training employees to recognize and respond to cybersecurity threats is crucial.

Real-Life Example: A company runs phishing simulations to educate employees on identifying phishing attempts.

Tip for Firms:

— Phishing Simulations: Regularly run simulated phishing campaigns to assess employee vigilance and improve awareness.

7. Incident Response and Recovery

A structured Cyber Incident Response Plan ('CIRP') helps mitigate the impact of a cyber incident and facilitates quick recovery.

Real-Life Example: Following a ransomware attack, a company activates its CIRP, restores backups, and communicates with affected customers.:

Tip for Firms:

— Create a Detailed CIRP: Develop a comprehensive response plan with defined roles and procedures for handling cyber incidents.

8. Communication and Notification

Timely and clear communication during a cyber incident is essential for managing stakeholder expectations.

Real-Life Example: After a data breach, a company notifies relevant parties within 72 hours as per a predefined communication plan.

Tip for Firms:

— Pre-approved Communication Templates: Create templates for various scenarios to ensure quick and consistent messaging.

9. Continuous Improvement

Cybersecurity requires ongoing efforts to stay ahead of evolving threats. Regular testing, assessments, and reviews help maintain effective security measures.

Real-Life Example: After a penetration test, a company addresses weaknesses and continues testing annually.

Tip for Firms:

— Penetration Testing: Conduct regular tests to identify vulnerabilities and improve your cybersecurity posture.

10. General Practices for Enhancing Cybersecurity

Consider the following practices to strengthen your cybersecurity strategy:

— Conduct Regular Security Audits: Regularly test your systems for vulnerabilities.
— Implement Strong Access Controls: Use least privilege and multi-factor authentication for sensitive data.
— Train Employees: Regularly educate staff on identifying phishing attacks and secure browsing practices.

What Next?

As DFSA-authorised firms work to align their cybersecurity efforts with GEN Rule 5.5 on Cyber Risk Management, building a culture of proactive security is crucial.

At Waystone, our Cybersecurity Team can assist with a range of services, including gap analysis, policy creation, and security awareness training. Contact us today to strengthen your cybersecurity resilience and ensure full regulatory compliance.

Contact Us →