PENTA

DFSA CYBER RISK COMPLIANCE ROADMAP

By Penta

2025

Improve your cyber risk compliance based on the latest guidelines published by the DFSA, focusing on what it identifies as the most common and crucial areas for improvement.

Content

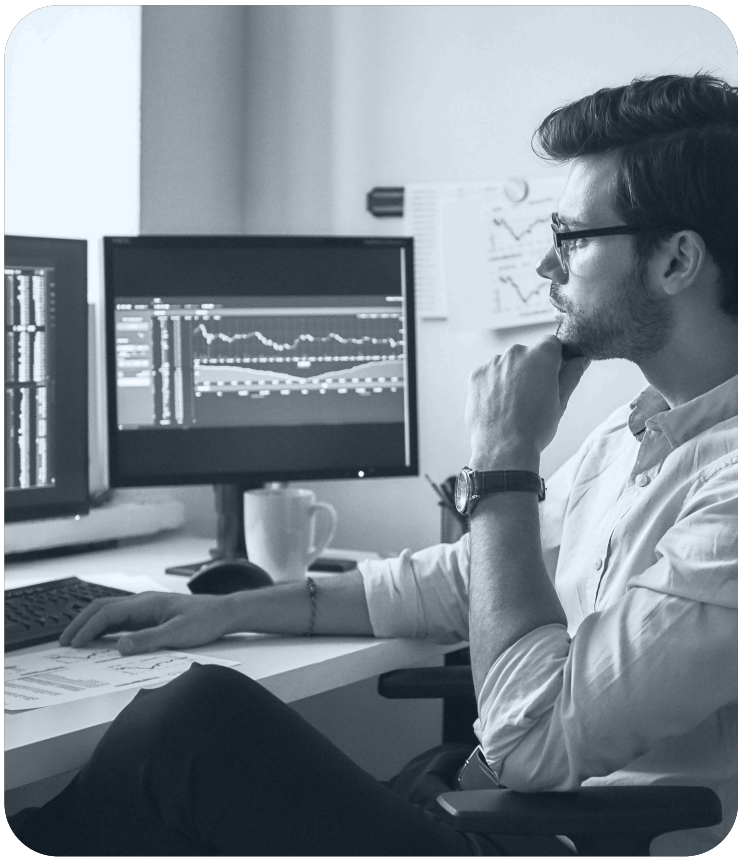
Overview

Overview

According to the latest M-Trends threat intelligence **report by Mandiant,** the financial services sector is one of the most targeted by cybercriminals.

Cyber risk management is a key priority for the DFSA, especially since the global pandemic and the ensuing spike in cyber-criminal activity worldwide.

In their Cyber Thematic Review 2024, the DFSA emphasised the importance of proactive planning, training, and monitoring to safeguard against cyber threats.



As part of this, firms must create and maintain a thorough cybersecurity training programme to ensure relevant employees understand cybersecurity policies, develop the skills to detect and report cyber incidents, and understand their personal responsibilities. Firms should also have a programme to annually – if not more regularly – test the strength of their IT systems, networks, and controls, addressing any issues uncovered.

The DFSA also underscored the importance of completing regular IT compliance audits, highlighting that currently, companies in the DIFC are not fully completing these audits with every area up to standard.
It have provided a set of guidelines as best practices for firms to adopt.

Outlook for 2025

Outlook for 2025

Cybersecurity remains a key focus for DFSA-regulated firms in 2025. By adhering to the DFSA's cyber risk management rules and addressing the identified priorities, firms can enhance their defences against cyber threats, safeguarding their operations, clients, and the broader financial ecosystem.

Regulated firms are encouraged to strengthen governance by implementing robust cyber risk frameworks, maintaining accurate IT asset inventories, and ensuring third-party providers meet stringent cybersecurity standards. Additionally, improving encryption practices, conducting regular system tests, and enhancing incident response planning will be essential for building resilience. By fostering employee awareness and participating in information-sharing platforms, firms can stay prepared for the evolving cyber threat landscape.

What are the DFSA’s cyber risk guidelines and who do they apply to?

What are the DFSA's cyber risk guidelines and who do they apply to?

The DFSA began publishing its Cyber Risk Management Guidelines in June 2024 to help regulated companies establish a robust IT security management framework.
These rules focus on three core areas: governance, cyber hygiene, and resilience. They guide firms in establishing strong risk management frameworks, securing IT systems with practices like encryption and regular testing, and preparing for incidents with effective detection, response, and recovery plans.

The DFSA monitors firms' compliance with these rules and evaluates whether they are improving their cybersecurity practices. Regular reviews and assessments ensure that firms align with the expectations set out in the rules.

These regulations apply to all **Authorised Firms, Registered Auditors, Credit Rating Agencies, and Authorised Market Institutions operating** in the Dubai International Financial Centre (DIFC). Firms that fail to comply with these rules may face penalties, suspension, or revocation of their licenses.

DFSA Cyber Security Compliance Initiatives – Timeline

DFSA Cyber Security Compliance Initiatives – Timeline

OCTOBER 2019

Launch of the online incident reporting portal for regulated companies to report cyber incidents.

JANUARY 2020

Launch of the cyber threat intelligence platform (DFSA TIP), which aims to encourage the development of information sharing among financial services companies. The TIP platform is available to authorised firms through the DFSA's ePortal.

JUNE 2020

First review report published evaluating the cyber security programmes of DFSA-regulated firms. Against the backdrop of a global pandemic and most firms switching to remote work, the report highlighted relevant opportunities for implementing best practices in cyber risk management.

DECEMBER 2020

Cyber Risk Management Guidelines published to help regulated companies in the DIFC establish a robust cyber security management framework. The guidelines cover 22 different areas related to governance, security practices, and protection against attacks.

JANUARY 2022

Second review report published showing significant improvement in cyber risk and governance practices in most areas. However, the report also showed little or no improvement in areas such as information sharing, incident response, vulnerability assessment, and IT asset management.

JANUARY 2024

Codified the Cyber Risk Management Guidelines into formal rules under the DFSA Rulebook. This provided a stronger regulatory foundation for cybersecurity practices across firms operating within the DIFC.

JUNE 2024

Third review report published showing progress in continuous monitoring, detection capabilities, and cyber hygiene. However, IT compliance, incident response testing, training programmes and threat intelligence are all areas that need to be improved.

2025

Continued periodic reviews, cybersecurity events and enhanced supervision of cyber risks.

Why is the DFSA doing this? Top Priorities for 2025

Why is the DFSA doing this?

The DFSA requires regulated companies to establish a strong cybersecurity framework and consistently enhance their capabilities to monitor, detect, and respond to security incidents.

The goal is to ensure companies can identify and prevent cyber threats while effectively managing and mitigating security incidents.

To help companies meet compliance requirements, the DFSA has put in place multiple tools:

- **Incident reporting mechanisms**
- **Threat intelligence platform**
- **Detailed guidelines on cyber risk management**
- **Regular reviews assessing overall compliance**
- **Company-specific cyber risk assessments**
- **Awareness workshops and roundtables**

Top Priorities for 2025

In 2024 the DFSA published its third review report, which showed significant improvement in continuous monitoring, detection capabilities, and cyber hygiene. However, **IT compliance, incident response testing, training programmes and threat intelligence are all areas that need to be improved.**

The priority areas for improvement highlighted by the report were mainly as follows:

- **Cyber Risk Management Framework**
- **Training and Cyber Awareness Campaigns**
- **IT Systems and Network Resilience Obligations**
- **Vulnerability Assessment and Penetration Testing**
- **IT Asset Identification and Classification**
- **Third-Party Risk Management**
- **Threat Monitoring, Detection and Response**
- **Encryption**

RECOMMENDED STEPS FOR DIFC BUSINESSES

Cyber Risk Management Framework

A cyber risk management framework provides a structured approach to managing cyber risks across an organisation. While the DFSA does not mandate the use of a specific framework or standard (acknowledging that no single solution fits all firms) it does highlight several relevant frameworks, with the most notable being:

The G7 Fundamental Elements of Cybersecurity for the financial sector, which provides foundational principles for enhancing cybersecurity practices.

The ISO/IEC 27000 series of standards, applicable to organisations of all sizes and industries, offering a comprehensive framework for information security management.

The CPMI-IOSCO GUIDANCE on cyber resilience for financial market infrastructures, specifically designed for sectors managing transactions, such as settlement and clearing systems.

Work with an expert to select the appropriate framework for your organisation and develop a structured plan for its implementation. **This typically includes:**

- **Setting the scope and objectives of your cyber risk management framework.**
- **Identifying and evaluating potential risks to your organisation's critical assets, systems, and data.**
- **Creating policies and procedures to effectively manage and reduce cyber risks.**
- **Assigning clear roles and responsibilities for cyber risk management throughout the organisation.**
- **Establishing a continuous risk management process that includes regular assessments, mitigation strategies, and communication.**
- **Designing incident response plans to efficiently handle potential cyber-attacks and data breaches.**

Training and Cyber Awareness Campaigns

The vast majority of cyber attacks on businesses occur due to employees' lack of awareness about cyber risks. Training and awareness campaigns are essential to help employees understand the dangers of cyber threats and their responsibility in safeguarding the organisation's systems and data.

Effective cybersecurity awareness is an ongoing effort, not a one-time exercise. Awareness initiatives should aim to ensure that employees at all levels understand their role in maintaining cybersecurity and are equipped to identify and respond to potential threats. To achieve this, Penta advocates for the implementation of an ongoing cyber awareness training programme.

CLAUSE 5.5.14 OF THE DFSA GENERAL RULEBOOK SPECIFICALLY REQUIRES STAFF TRAINING TO BE CONDUCTED. IT SAYS:

1) An Authorised Person must establish and maintain a comprehensive cybersecurity training programme and adequate awareness arrangements.

(2) The programme and arrangements in (1) must ensure that all relevant Employees:

(a) Receive training, at least annually, on the Authorised Person's cybersecurity policies and standards;

(b) Develop and maintain appropriate awareness of, and competencies for, detecting and reporting Cyber Incidents; and

(c) Understand their individual responsibilities.

Key Strategies To Enhance Your Cyber Awareness Programme

- Partner with a cybersecurity training provider with expertise in your industry.
- Create a comprehensive training programme that includes both general awareness and role-specific modules tailored to employees' responsibilities.
- Schedule regular training sessions to reinforce key principles and keep employees informed about emerging threats and best practices.
- Incorporate simulated phishing attack campaigns to assess the programme's effectiveness. Tools like Microsoft Defender Plan 2 and KnowBe4 offer excellent resources, combining security awareness content with phishing simulations and analytics.
- Encourage employees to report potential security threats and provide a mechanism for doing so anonymously if desired.
- Ensure senior management is fostering a culture of cybersecurity awareness to support employees.

Cybersecurity Training and Awareness as a Top Priority for 2025

According to the DFSA Rulebook: An Authorised Person is required to implement and maintain a robust cybersecurity training programme alongside adequate awareness measures.

These initiatives must ensure that all relevant employees:

- **Receive annual training on the organisation's cybersecurity policies and standards.**
- **Develop and sustain the necessary awareness and skills to detect and report cyber incidents effectively.**
- **Understand their individual responsibilities in protecting the organisation's systems and data.**

Additionally, an Authorised Person must ensure that their organisation has a comprehensive programme for testing the resilience of its IT systems, networks, and associated controls.

This programme MUST INCLUDE:

- **Regular vulnerability assessments**
- **Scenario-based testing**
- **Penetration testing**
- **Red team exercises**

For systems exposed to the internet, testing must occur at least annually. Furthermore, the organisation must establish a process to prioritise and address any vulnerabilities or weaknesses identified during testing.

IT Systems and Network Resilience Obligations

The DFSA emphasises a regulated company's ability to identify and evaluate potential risks to its systems and data, assess the likelihood and potential impact of those risks, and implement appropriate mitigation strategies.

Recommendations for identifying and evaluating cyber risks in your organisation:

- **Implement a comprehensive programme to evaluate the resilience of all IT systems, networks, and data.**
- **Identify potential threats and vulnerabilities to these systems and assess their likelihood and potential impact.**
- **Evaluate the effectiveness of current controls and mitigation strategies.**
- **Prioritise and address adverse testing results promptly.**
- **Mitigate risks based on their assessed likelihood and potential impact.**
- **Develop a risk management plan that outlines appropriate mitigation strategies for each identified risk.**
- **Conduct regular testing under the programme, with internet-facing systems tested at least annually.**

Categorising different types of threats is essential for identifying the appropriate mitigation strategies for each. For instance, the measures used to mitigate ransomware attacks differ significantly from those needed for insider threats, third-party risks, or natural disasters.

IT Systems and Network Resilience Obligations

The DFSA adds: that an Authorised Person must ensure that:

- **It has in place a comprehensive programme to test the resilience of its IT Systems and Networks and its processes and controls implemented to comply with Rules 5.5.6 to 5.5.14;**
- **Testing under the programme is carried out regularly, and in the case of internet-facing systems, at least annually; and**
- **It has in place a process to prioritise and remedy adverse testing outcomes.**

Furthermore, **an Authorised Person should use a range of methods to test its IT Systems and Networks, as well as processes and controls,** including:

- Vulnerability assessments;
- Scenario-based testing;
- Penetration tests; and
- Red team exercises.

It specifically adds that **"the frequency with which an Authorised Person should carry out testing will depend on the nature, scale and complexity of its business.**

"For some Authorised Persons, it may be adequate to test annually, but for others, it may be necessary to carry out tests more frequently.

The DFSA expects additional tests to be carried out whenever systems are updated or new systems are implemented, including when systems are changed to address any vulnerabilities identified during testing."

Vulnerability Assessment and Penetration Testing

Performing vulnerability assessments and penetration testing allows your organisation to proactively identify and address security risks before attackers can exploit them.

Partner with reputable and experienced third parties to conduct these assessments and tests regularly, identifying potential weaknesses in your systems and networks.

Leverage the results to evaluate the effectiveness of your current security controls.

Create and execute a remediation plan to resolve identified vulnerabilities and strengthen your defences.

IT Asset Identification and Classification

This area is frequently overlooked, even though it's relatively easy to manage and extremely important. IT asset identification and classification involve systematically identifying and organising your organisation's hardware, software, and data assets.

A good place to start is by leveraging data from your finance department, as it usually maintains records of all purchases. The more challenging aspect is tracking employees' personal devices. One effective method is to use admin dashboards from key tools like email and applications, which often provide logs of connected devices and active sessions.

Recommendations:

- **Create a comprehensive asset inventory that includes all hardware, software, and data assets within your organisation.**
- **Appoint a Data Protection Officer (DPO) to ensure your organisation processes, stores and handles data in compliance with DIFC's data protection rules.**
- **Categorise assets based on their importance to the organisation and the potential consequences of their loss or compromise.**
- **Establish a data classification system that defines the sensitivity and confidentiality levels of different types of data.**
- **Give special attention to employees' personal devices (BYODs – Bring Your Own Device), as they are often more susceptible to vulnerabilities.**
- **Apply appropriate security controls to each asset according to its classification and criticality.**
- **Ensure you perform regular audits of your asset inventory to ensure it remains current and accurate.**

Third-Party Risk Management

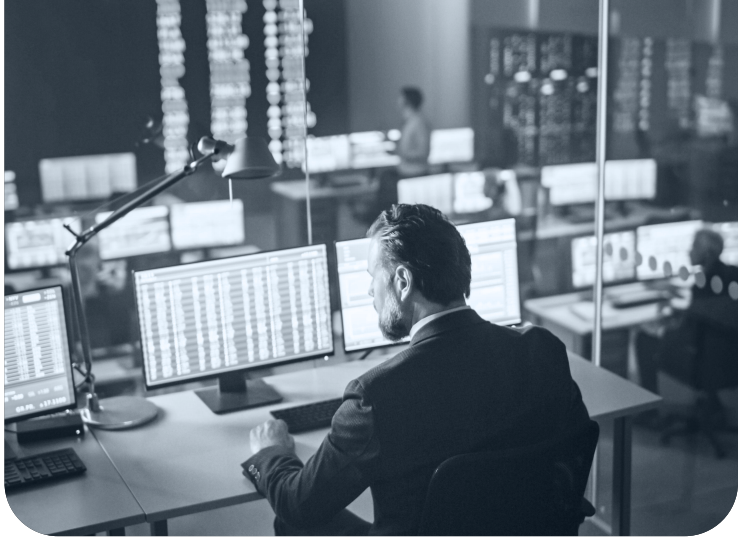
Engaging with third parties, such as suppliers and contractors, can heighten your organisation's exposure to cyber risks and pose significant threats to the security of sensitive data and operations. The DFSA expects regulated firms to address these risks by implementing robust mitigation strategies and maintaining readiness to manage potential vulnerabilities.

Recommendations for managing third-party cyber risk:

- **Establish a comprehensive third-party risk management programme that incorporates a risk assessment process, due diligence requirements, and continuous monitoring and evaluation.**
- **Identify all third-party vendors, suppliers, and contractors, particularly those with access to your systems, networks, or data.**
- **Evaluate the risks associated with each third-party relationship by considering the sensitivity of the data or systems they access and the potential impact of a breach or compromise.**
- **Create and implement contract terms that obligate third-party vendors to comply with your organisation's security standards and reporting requirements.**
- **Continuously monitor third-party vendors to ensure adherence to your security standards, and conduct regular audits and assessments to uncover potential vulnerabilities or risks.**

Threat Monitoring, Detection, and Response

An organisation cannot effectively protect itself from cyber threats without the appropriate technology and tools to monitor, detect, and respond to these risks.



Recommendations for effective threat monitoring, detection and response:

- **Deploy a robust threat monitoring system that combines automated and manual monitoring, typically through a Security Information and Event Management (SIEM) platform managed by an in-house or outsourced Security Operations Center (SOC).**
- **Establish detailed incident response plans that outline roles, responsibilities, and step-by-step guidance for addressing potential threats and attacks.**
- **Perform regular security audits and vulnerability assessments to uncover and address weaknesses in your systems and networks.**
- **Leverage threat intelligence sources to stay informed about emerging threats and attack methods. SIEM solutions often integrate multiple intelligence sources to enhance threat detection and response capabilities.**
- **Implement a robust access control system to safeguard your systems and data from unauthorised access.**

The DFSA's General Rulebook recommends the regular review required by Rule 5.5.17(4). This should take into account current cyber threat intelligence, as well as lessons learned from previous events and be adjusted to account for new processes and services. Where the review is triggered by a major Cyber Incident (see Guidance item 1 under Rule 5.5.19), **the DFSA expects an Authorised Person to assess whether established procedures were followed and whether actions taken were effective.** It should also identify key lessons learnt with a view to improving future Cyber Incident response and recovery processes.

Encryption

Encryption is a vital method for safeguarding your data against unauthorised access or disclosure.

Recommended actions for using encryption in your organisation:

- **Apply robust encryption protocols to protect all sensitive data, whether it is in transit or at rest.**
- **Use industry-standard encryption algorithms like AES-256 and RSA, paired with effective cryptographic key management practices to maintain data security.**
- **Enhance the protection of encrypted data by implementing multi-factor authentication for access.**

> Cyberattacks are a serious and costly threat that is rapidly increasing. IT security must be a top priority. Failure to address this adequately could result in severe consequences, either through regulatory action or exploitation by cybercriminals, potentially jeopardising your business.

Lester Pinto
Regional Manager, Penta

Connect on Linkedin

> Compliance with the DFSA's rules is not just a regulatory requirement but a critical foundation for building robust cybersecurity practices. This is paramount for protecting your organisation, its clients, and the broader financial ecosystem from ever-evolving threats, while ensuring the highest standards of data protection and confidentiality.

Mohammad Hammoudeh
Information Security Specialist, Penta

Connect on Linkedin

Further Reading

- DFSA Cyber Risk Management Guidelines
- DFSA Cyber Thematic Review of 2024
- DFSA Rulebook
- G7 Fundamental Elements of Cyber Security for the Financial Sector
- ISO/IEC 27001:2022