PENTA

IT COMPLIANCE PLAYBOOK FOR FSRA-REGULATED FIRMS

Everything ADGM businesses need to align with FSRA's IT and cybersecurity requirements.

2025

Contents

Introduction

Introduction

- **Purpose of the guide**
- **Who this guide is for (authorised firms, financial institutions, legal entities in ADGM)**
- **Importance of IT compliance in ADGM:** compliance-driven vs. value-driven markets
- **FSRA's role and regulatory environment overview**

As the regulatory landscape in Abu Dhabi Global Market (ADGM) continues to mature, firms operating under the Financial Services Regulatory Authority (FSRA) must ensure their IT infrastructure and cybersecurity practices meet stringent compliance obligations.

ADGM has introduced a comprehensive standalone IT Risk Management Guidance in addition to the cyber-risk requirements defined in the FSRA General Rulebook.

This guide provides FSRA-regulated firms with a practical roadmap to IT compliance, focused on risk management, governance, and operational readiness.

At Penta, we support regulated financial and professional services firms by delivering IT audit services, cyber security expertise with CISO-level experience and competencies, cybersecurity training, and managed infrastructure built for ADGM's compliance expectations.

Regulatory Framework Overview

Regulatory Framework Overview

- **Overview of the FSRA General Rulebook (GEN), especially Chapter 3 – IT-related requirements**
- **Summary of Information Technology Risk Management Guidance (Nov 2024)**
- **Key linked regulatory areas: Data protection, Cybersecurity, IT governance**

ADGM's FSRA requires regulated entities to comply with two key frameworks that collectively define the standards for IT governance and cybersecurity resilience:

FSRA General Rulebook (GEN) –

Chapter 3 of the General Rulebook outlines 42 IT-related control requirements that all firms must implement. These range from IT governance and audit to system access control, change management, and user awareness.

The controls are broad in scope and designed to ensure that IT infrastructure supports safe and sound business operations in a regulated environment.

FSRA IT Risk Management Guidance (November 2024) –

This standalone guidance expands upon the principles in the General Rulebook by providing a risk-based methodology for identifying, assessing, and mitigating IT risks.

It covers areas such as cyber risk governance, operational resilience, vendor risk management, and incident response. Together, these frameworks form a clear, enforceable baseline for IT compliance within ADGM.

At Penta, we use both documents to conduct structured gap assessments, build prioritised compliance plans, and deliver managed services that help firms stay aligned with FSRA expectations throughout their lifecycle.

Core FSRA IT Compliance Requirements

Core FSRA IT Compliance Requirements

IT Audit (GEN 3.3.13–3.3.15)

- **Requirements for internal IT audit**
- **Audit cycles, reporting, independence**
- **Common non-compliance risks**

Firms must conduct regular internal IT audits to assess the design and effectiveness of their systems, controls, and governance processes.

These audits must be clearly documented, reviewed by management, and made available upon FSRA request.

Audit requirements include a defined audit cycle – typically annual – with ad hoc reviews following significant changes to systems or risk posture.

Firms must ensure that audits are conducted independently, either by an internal team with no operational responsibility or through an external provider. Reports should include risk-ranked findings and a remediation plan with assigned owners and deadlines.

Common non-compliance risks include failing to follow up on audit findings, inadequate change tracking, and incomplete documentation of IT governance processes.

FSRA places strong emphasis on traceability and evidence of continuous improvement, making audit readiness an essential pillar of IT compliance.

Cybersecurity Awareness and Training (GEN 3.3.19)

- **Mandatory employee training programmes**
- **Recommendations for frequency and scope**
- **Measuring effectiveness (e.g. phishing simulations)**

Cybersecurity training is a mandatory compliance requirement under FSRA.

Firms must implement structured, ongoing awareness programmes that educate employees about current threats, secure behaviour, and regulatory obligations.

These programmes must be documented and regularly updated to reflect emerging risks.

Training should be delivered at least annually, with additional sessions during onboarding and after significant policy or system changes. Content should be tailored by role to address relevant security responsibilities and exposures.

Effectiveness should be measured through testing and simulations—particularly phishing exercises—to identify knowledge gaps and track progress over time.

FSRA expects firms to be able to demonstrate not only that training is delivered, but that it is effective in reducing risk.

IT Governance and Controls (GEN Chapter 3 overall)

- **Board and senior management responsibility**
- **Documentation and record keeping**
- **Segregation of duties, change management, and vendor oversight**

Firms must implement a clear, documented IT governance framework that enforces accountability and ensures IT-related risks are identified and managed.

FSRA expects governance structures to be regularly reviewed and applied consistently across internal teams and third-party providers, with an emphasis on robust documentation and accessible record keeping.

Responsibility for IT risk and governance must rest with the board and senior management.

These individuals must be able to demonstrate not only their oversight role but also their understanding of the firm's infrastructure, exposure to operational risks, and its compliance posture.

Documentation of decisions, risk assessments, and IT strategy reviews is critical.

Operational integrity must be safeguarded through segregation of duties and formalised change management processes, ensuring that no single individual has end-to-end control over critical systems.

Change controls should be documented, approved, and logged to provide full traceability.

Vendor oversight is another key requirement. Firms must maintain a current register of third-party providers, conduct formal risk assessments, and ensure contracts contain explicit terms regarding service levels, compliance obligations, and audit rights.

These measures ensure that outsourcing does not compromise regulatory accountability.

FSRA IT Risk Management Guidance (2024)

FSRA IT Risk Management Guidance (2024)

- **Role of risk-based approach in IT strategy**
- **Key domains:**
  - **Risk identification and assessment**
  - **Incident response and resilience planning**
  - **Vendor and third-party risk**
  - **Asset management and classification**
  - **Monitoring and testing**

The IT Risk Management Guidance (2024) guidance supplements the General Rulebook and provides a risk-based model to evaluate, plan, and execute IT strategies.

Key domains include:

Risk identification & classification

Mapping of assets, systems, and business functions to risk categories.

Incident response and resilience

Firms must document and test their incident response and disaster recovery plans regularly.

Third-party risk

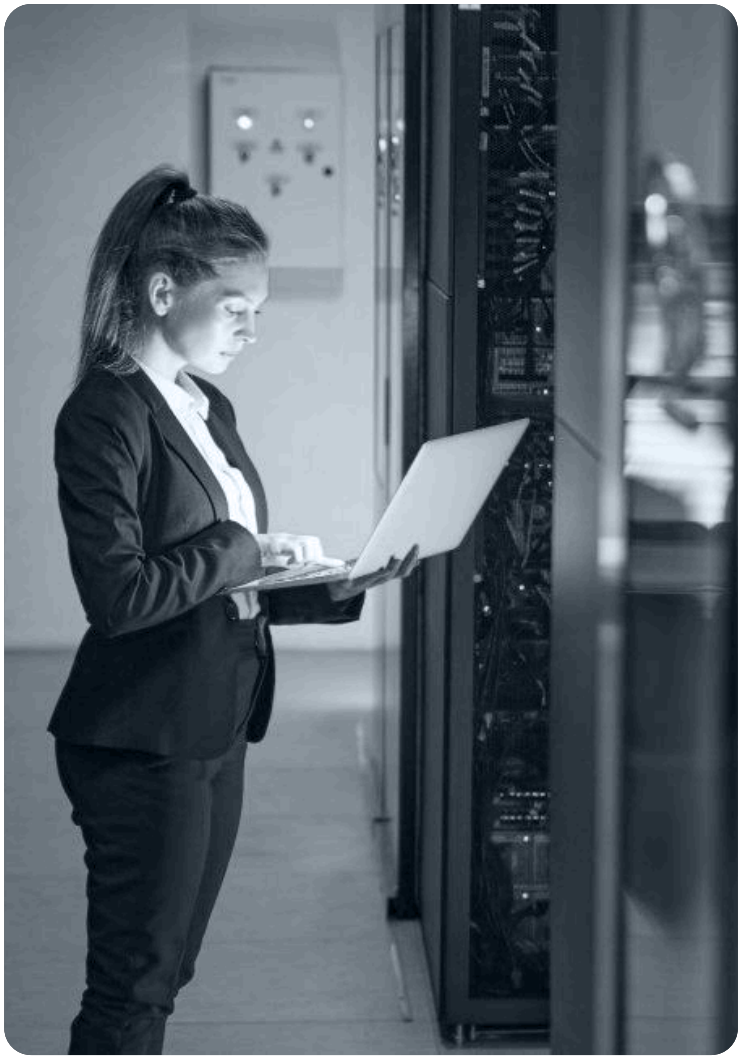
Outsourced service providers must be assessed and reviewed against defined security and compliance benchmarks.

Monitoring and testing

Continuous controls monitoring, vulnerability scanning, and periodic assessments are required.

Data Protection Obligations

Data Protection Obligations



- **ADGM data protection regulations**
- **Cross-border data transfer restrictions**
- **Recommended data governance practices**

The FSRA compliance ecosystem incorporates ADGM's data protection regulations, which are legally binding on all entities processing personal data within ADGM.

These rules emphasise lawful and transparent processing, data subject rights, and clear governance around how personal information is stored, accessed, and shared.

Organisations must implement robust data governance practices, including asset classification, access control, and purpose-limited data usage.

Data transfers outside the UAE are only permitted under strict conditions and require contractual safeguards or regulatory approval.

In practice, this means firms must map their data flows and assess third-country protections before moving personal data offshore.

In addition, firms must develop and test incident response plans that include breach detection, notification, and remediation procedures.

It is important not to conflate data protection with cybersecurity—**FSRA examiners expect both to be addressed independently,** each with its own controls, documentation, and accountability structures.

How Penta Helps

How Penta Helps

- **Overview of Penta's managed IT services aligned with FSRA requirements**
  - **Internal IT audits**
  - **Cyber awareness training (KnowBe4, phishing campaigns)**
  - **vCISO services**
  - **Incident response and business continuity planning**
- **Track record in DIFC and readiness for ADGM**

PENTA PROVIDES A COMPLETE SUITE OF MANAGED SERVICES ALIGNED WITH FSRA COMPLIANCE:

Internal IT audit support

Audit preparation, control documentation, and gap remediation

Cybersecurity training

Managed awareness campaigns, learning management system (LMS) integration, and phishing simulations

Virtual CISO services

Strategic guidance, policy development, and FSRA liaison support

Secure hosting & monitoring

ISO-certified environments with 24/7 incident response

Penta's expertise spans multiple regulatory environments, including FSRA (ADGM), DFSA (DIFC), FINMA (Switzerland), DORA (EU), the SEC and PRA (US/UK), and compliance regimes in Saudi Arabia such as SAMA and ECC.

Penta has maintained ISAE 3402 Type II certification since 2008 and operates **ISO 27001:2022-certified infrastructure**, ensuring independently audited governance and risk controls across its services.

With this experience, Penta ensures that its IT services are always mapped to applicable regulations, helping firms across jurisdictions meet audit expectations while maintaining operational resilience and security.

Implementation Roadmap

Implementation Roadmap

Step-by-step compliance onboarding process:

1 Gap assessment

2 Control mapping

3 Policy development

4 Technology implementation

5 Training and audit preparation

1 INITIAL GAP ASSESSMENT

Evaluate current state vs. GEN and Risk Guidance requirements through structured interviews, document reviews, and system scans. Identify gaps in policy, procedure, technology, and governance, and prioritise based on risk exposure and regulatory urgency.

2 CONTROL MAPPING

Align existing and missing controls to the 42 GEN requirements and broader FSRA Risk Management domains. This includes mapping technical controls (e.g. access restrictions), administrative controls (e.g. policy approvals), and operational practices to demonstrate full coverage.

3 POLICY AND TRAINING ROLLOUT

Develop or revise information security and IT governance policies based on mapped requirements. Deliver tailored training programmes to ensure that staff understand their roles and responsibilities, and that records of participation and completion are retained.

4 TESTING & AUDIT PREP

Implement control testing procedures and conduct mock audits to validate documentation, process execution, and traceability. Address any remaining deficiencies and prepare audit packs to satisfy FSRA inspection readiness.

5 ONGOING MONITORING

Deploy and maintain tools for continuous compliance monitoring, such as endpoint detection, access logs, and patch tracking. Use dashboards and reports to demonstrate sustained compliance and support regulatory change management.

FAQs

FAQs

How often must we conduct an IT audit?

Annually or more frequently if material changes occur.

What qualifies as compliant cybersecurity training?

Ongoing, documented training that includes awareness of phishing, data handling, and policy onboarding.

Can Penta act as our outsourced CISO?

Yes. Penta provides vCISO services tailored to FSRA-regulated businesses.

Should data protection be covered in our cybersecurity strategy?

No. FSRA expects firms to treat data protection and cybersecurity as distinct, separately governed domains.

Do we need to document cybersecurity incidents even if they're minor?

Yes. All incidents, regardless of severity, should be logged with clear timestamps, outcomes, and follow-up actions. FSRA places strong emphasis on traceability and continuous improvement.

How does FSRA evaluate third-party vendor risk?

Firms must assess third-party providers regularly, maintain an up-to-date vendor register, and ensure all contracts include appropriate SLAs, data protection clauses, and audit rights.

What is the role of the board in IT compliance?

The board and senior management bear ultimate responsibility for IT risk governance. FSRA expects them to demonstrate oversight and approve IT strategy and risk controls.

Can compliance controls be automated?

Yes. Automated tools for patching, access control, monitoring, and reporting are recommended—provided they are supported by documented processes and regular reviews.

Further reading

- FSRA General Rulebook – Chapter 3 (GEN 3.3)
- FSRA IT Risk Management Guidance – 20 November 2024
- ISO/IEC 27001 Training Requirements Reference
- NIST Special Publication 800-61 Revision 2 – Computer Security Incident Handling Guide