



 Abu Dhabi Global Market - Financial Services Regulatory Authority

ADGM FSRA Compliance Map

Complete Guide to Technology Risk Management
Requirements for Financial Institutions & Crypto
VASPs

Edition: 2026

Executive Summary

Understanding ADGM FSRA compliance for financial services in Abu Dhabi

| What is ADGM FSRA Compliance?

The Abu Dhabi Global Market Financial Services Regulatory Authority (ADGM FSRA) regulates financial services in ADGM, including banks, investment firms, and crypto asset service providers (VASPs). FSRA's Technology Risk Management framework mandates comprehensive cybersecurity controls, operational resilience, and specific requirements for firms handling virtual assets. ADGM has positioned itself as a leading crypto hub, requiring robust security for digital asset custody, trading, and smart contracts.

Key Insight: ADGM is one of the most crypto-friendly jurisdictions with clear regulatory guidance. All regulated entities must implement robust technology risk management and demonstrate ongoing compliance through regular testing and reporting.

| Who Needs ADGM FSRA Compliance?

The following entities operating in Abu Dhabi Global Market must comply with FSRA Technology Risk requirements:

 Banks & Credit Institutions

 Investment Firms

 Asset Managers

 Insurance Companies

 Crypto VASPs

 Custody Providers

 Crypto Exchanges

 Trading Platforms

⚠ Regulatory Expectations: FSRA expects annual independent penetration testing for all material systems. High-risk entities (exchanges, large banks) should conduct more frequent testing, typically semi-annually or quarterly.

Core Requirements Matrix

ADGM FSRA Technology Risk Management requirements mapped to ITSEC solutions

#	Category	Requirement	Description	ITSEC Solution
1	Governance	Technology Risk Governance	Board oversight, CISO appointment, and risk appetite statements	vCISO & Framework Design
2	Access	Access & Authentication	MFA, privileged access management, and identity governance	IAM & PAM Solutions
3	Data	Data Protection	Encryption, DLP, secure data handling, and data residency	Data Security Framework
4	Network	Network Security	Segmentation, perimeter defense, and intrusion detection	Network Penetration Testing
5	Crypto	Crypto Asset Security	Hot/cold wallets, custody, and smart contract audits (VASPs)	Crypto Security Testing
6	Incident	Incident Management	FSRA notification, IR procedures, and forensics capability	IR Planning & Tabletops

ITSEC Advantage: With 70+ ADGM entities served and 100% FSRA compliance rate, our team understands the specific technology risk expectations of Abu Dhabi's financial regulator.

Extended Requirements Matrix

Additional technology risk and cybersecurity controls required by ADGM FSRA

#	Category	Requirement	Description	ITSEC Solution
7	Third-Party	Third-Party Risk	Vendor assessments, cloud security, and API integration review	Vendor Security Audit
8	Testing	Regular Testing	Annual pen tests, vulnerability management, and red team exercises	VAPT & Red Team
9	Resilience	Operational Resilience	BCDR, high-availability systems, and business continuity planning	BCDR Testing
10	Change	Change Management	Controlled change management for systems and infrastructure	Change Control Advisory
11	Awareness	Security Awareness	Staff training, phishing simulations, and security culture	Training Programs
12	Audit	Audit & Logging	Comprehensive logging, SIEM integration, and audit trails	SOC & Monitoring

International Standards Recognized

FSRA recognizes ISO 27001, SOC 2, PCI DSS, and similar international standards as evidence of robust security practices. Many ADGM entities pursue these certifications.

Reporting Obligations

Licensed entities must notify FSRA of material cybersecurity incidents, maintain comprehensive audit trails, and submit annual technology risk assessments.



Your Path to ADGM Compliance

ITSEC's proven methodology gets you FSRA-ready efficiently

Week 1

Initial Consultation & Scoping

Comprehensive discovery session to understand your operations, license category, and current security posture against FSRA requirements.

Weeks 1-2

Technology Risk Assessment

Detailed gap analysis of your current state against all ADGM FSRA Technology Risk Management requirements. Deliverable: Gap Assessment Report.

Weeks 2-4

Security Testing (VAPT)

Comprehensive penetration testing of web applications, APIs, mobile apps, infrastructure, and crypto-specific systems (for VASPs).

Weeks 4-6

Remediation & Documentation

Fix identified vulnerabilities, develop required policies and procedures, implement technical controls, and prepare evidence packages.

Ongoing

Continuous Compliance

Quarterly vulnerability scanning, annual penetration testing, FSRA reporting support, and ongoing advisory services.

✓ **Final Outcome:** Full FSRA compliance — Operate with confidence in Abu Dhabi's premier financial center.

Entity-Specific Requirements

Tailored security solutions for each ADGM license category



Traditional Financial Institutions

- ✓ Core banking system security
- ✓ Trading platform penetration testing
- ✓ Wealth management platform security
- ✓ Mobile & internet banking testing



Crypto VASPs

- ✓ Hot wallet & cold storage audits
- ✓ Smart contract security (Solidity, Rust)
- ✓ MPC wallet implementation review
- ✓ Blockchain node & RPC security



Crypto Exchanges

- ✓ Exchange platform penetration testing
- ✓ Order matching engine security
- ✓ API security assessment
- ✓ KYC/AML system security



Custody Providers

- ✓ Vault security architecture
- ✓ Key management & HSM review
- ✓ Multi-signature protocols
- ✓ Asset transfer controls



Investment Firms

- ✓ Portfolio management systems
- ✓ Client portal security
- ✓ Trade execution platforms
- ✓ Reporting system integrity



Operational Resilience

- ✓ BCDR plan testing & tabletops
- ✓ Ransomware resilience simulation
- ✓ RTO/RPO achievement testing
- ✓ Crisis management assessment

Customized Approach: Each ADGM license category has specific technology risk requirements. ITSEC tailors our assessment methodology to address the unique security challenges of your business model.

ADGM FSRA Compliance Checklist

Self-assessment checklist for Technology Risk Management requirements

- | | |
|--|---|
| <input type="checkbox"/> Technology Risk Governance framework documented | <input type="checkbox"/> CISO or equivalent security function appointed |
| <input type="checkbox"/> Annual penetration testing completed | <input type="checkbox"/> Quarterly vulnerability scanning implemented |
| <input type="checkbox"/> Multi-factor authentication (MFA) enabled | <input type="checkbox"/> Privileged access management implemented |
| <input type="checkbox"/> Data encryption at rest and in transit | <input type="checkbox"/> Data loss prevention (DLP) controls |
| <input type="checkbox"/> Incident response plan documented and tested | <input type="checkbox"/> FSRA notification procedures established |
| <input type="checkbox"/> Business continuity plan in place | <input type="checkbox"/> Disaster recovery procedures tested |
| <input type="checkbox"/> Third-party vendor security assessments | <input type="checkbox"/> Cloud security controls validated |
| <input type="checkbox"/> Network segmentation implemented | <input type="checkbox"/> Intrusion detection/prevention systems |
| <input type="checkbox"/> Security awareness training completed | <input type="checkbox"/> Audit trail and logging implemented |
| <input type="checkbox"/> Wallet security audits (VASPs) | <input type="checkbox"/> Smart contract security review (VASPs) |

 **Important:** This checklist is for self-assessment purposes. FSRA expects independent verification of security controls. Contact ITSEC for a comprehensive technology risk assessment.

Why Choose ITSEC

Abu Dhabi's most trusted ADGM FSRA compliance partner



100% FSRA
Compliance Rate



ISO 27001
Certified



CREST
Accredited



12+ Years
in ADGM



Phone

+971.4.257.2406



Mobile

+971.52.509.7278



Email

hello@itsecnow.com

Ready to Get ADGM Compliant?

Schedule your free FSRA Technology Risk Assessment with our security experts today.

[Request Assessment →](#)

| Our ADGM Expertise

70+ ADGM entities served including 30+ crypto VASPs. Our team includes specialists in traditional finance and blockchain security with deep regulatory knowledge.

| Ongoing Support

We provide continuous compliance support including quarterly testing, annual assessments, FSRA reporting assistance, and regulatory change management.