DUBAI INTERNATIONAL FINANCIAL CENTRE

DFSA Cybersecurity Compliance Map

Operational Risk & Cyber Resilience Framework

Comprehensive mapping of DFSA Chapter 7 operational risk requirements to ITSEC cybersecurity solutions for DIFC-licensed financial institutions.

6	35+	100%
KEY AREAS	CONTROLS	COVERAGE

Section 01

Understanding DFSA Cybersecurity Requirements

⚖️ Dubai Financial Services Authority Overview

The Dubai Financial Services Authority (DFSA) is the independent regulator of financial services conducted in or from the Dubai International Financial Centre (DIFC). The DFSA's Operational Risk rulebook (Chapter 7) and supplementary Cyber Resilience guidance establish comprehensive cybersecurity requirements for all DIFC-licensed entities including banks, investment firms, asset managers, and FinTech platforms.

DFSA compliance requires robust information security governance, access controls, business continuity planning, incident response capabilities, and regular independent security testing. Non-compliance can result in significant penalties, license restrictions, or revocation.

500+
LICENSED FIRMS

Annual
PEN TEST REQUIRED

24hrs
INCIDENT REPORTING

Board
LEVEL OVERSIGHT

📋 Who Must Comply?

- Banks & Credit Institutions
- Investment Firms & Fund Managers
- Insurance Companies & Intermediaries
- Exchanges & Clearing Houses
- Payment Service Providers
- FinTech & Crowdfunding Platforms

⚠️ Non-Compliance Penalties

- Regulatory fines up to $10M+
- Public censure & reputational damage
- License conditions or restrictions
- Enhanced supervision requirements
- Personal liability for senior management
- License revocation in severe cases

Section 02

DFSA Chapter 7 Requirements Mapping

DFSA Requirement	Description	ITSEC Solution	Priority
GEN 5.3.22 Information Security Governance	Board-approved security policies, CISO function, and governance framework	vCISO Services, Policy Development, Governance Assessment	CRITICAL
GEN 5.3.23 Access Control Management	Strong authentication, privilege management, and access reviews	IAM Assessment, MFA Implementation, Access Audit	CRITICAL
GEN 5.3.24 Data Protection Controls	Encryption, DLP, and secure handling of customer data	Data Security Assessment, Encryption Review, DLP Strategy	HIGH
GEN 5.3.25 Security Testing	Annual penetration testing and vulnerability assessments	Penetration Testing, VAPT, Application Security	CRITICAL
GEN 5.3.26 Business Continuity	BCP/DRP planning, testing, and recovery capabilities	BCP Development, DR Testing, Resilience Assessment	HIGH
GEN 5.3.27 Incident Response	Incident detection, response procedures, and DFSA notification	IR Planning, Tabletop Exercises, Incident Support	CRITICAL
GEN 5.3.28 Third-Party Risk	Vendor due diligence and ongoing monitoring requirements	TPRM Framework, Vendor Assessments, Contract Review	HIGH

🔍 DFSA Regulatory Focus Areas for 2026

Cyber Resilience: Enhanced testing requirements including threat-led penetration testing (TLPT) for systemically important firms

Cloud Security: Specific controls for cloud outsourcing with concentration risk monitoring

AI & Automation: Governance requirements for algorithmic trading and AI-driven decisions

Supply Chain: Extended third-party risk requirements for critical service providers

Section 03

ITSEC DFSA Compliance Solutions

Penetration Testing

Annual DFSA-compliant pen testing for infrastructure, applications, and trading platforms

Gap Assessment

Comprehensive DFSA Chapter 7 gap analysis with prioritized remediation roadmap

vCISO Services

Experienced security leadership for board reporting and governance oversight

Policy Framework

DFSA-aligned security policies, procedures, and standards development

BCP/DR Testing

Business continuity validation, DR drills, and resilience scenario testing

Incident Response

IR planning, tabletop exercises, and regulatory notification support

🎯 DFSA Compliance Engagement Packages

Package	Scope	Duration	Ideal For
Essential	Annual pen test + gap assessment + remediation guidance	4-6 weeks	Category 4 firms, FinTech startups
Professional	Essential + policy development + BCP review + quarterly advisory	8-12 weeks	Category 3 firms, asset managers
Enterprise	Professional + vCISO + red team + continuous monitoring + DFSA liaison	Ongoing	Banks, exchanges, Category 1-2 firms

Section 04

DFSA Compliance Timeline

12-Week DFSA Compliance Journey

1-2
Discovery
Initial assessment, scoping, and stakeholder alignment

3-4
Assessment
Gap analysis, pen testing, and vulnerability assessment

5-8
Remediation
Control implementation, policy development, and fixes

9-10
Validation
Retest, BCP drill, and evidence collection

11-12
Reporting
Board presentation, DFSA documentation, and handover

Annual Compliance Calendar

Q1: Annual pen test, policy review
Q2: BCP/DR testing, risk assessment
Q3: Third-party reviews, training
Q4: Board reporting, audit prep

Quick Wins (First 30 Days)

- Complete asset inventory update
- Verify MFA on all critical systems
- Review incident response contacts
- Update security awareness training

DFSA Examination Readiness

DFSA conducts periodic thematic reviews and on-site examinations. ITSEC prepares firms for:

- **Document Review:** Complete policy and procedure packages ready for inspection
- **Mock Examinations:** Simulation of DFSA on-site review process
- **Evidence Files:** Organized compliance artifacts demonstrating control effectiveness
- **Board Preparedness:** Senior management interview coaching and preparation

Section 05

Technical Security Controls Matrix

Control Domain	DFSA Expectation	Technical Controls	Testing Method
Network Security	Segmentation, monitoring, intrusion detection	Firewalls, IDS/IPS, SIEM, network segmentation	Network pen test, config review
Application Security	Secure SDLC, vulnerability management	WAF, SAST/DAST, secure coding standards	Application pen test, code review
Identity & Access	Strong authentication, least privilege	MFA, PAM, IAM, SSO, access reviews	IAM assessment, privilege audit
Data Protection	Encryption at rest and in transit	TLS 1.3, AES-256, key management, DLP	Encryption review, data flow analysis
Endpoint Security	Malware protection, device management	EDR, MDM, patch management, hardening	Endpoint assessment, vulnerability scan
Cloud Security	Secure cloud configuration, monitoring	CSPM, CWPP, cloud-native controls	Cloud security assessment, config audit

Penetration Testing Scope

- External infrastructure testing
- Internal network assessment
- Web application testing
- Mobile application review
- API security assessment
- Social engineering (optional)

Continuous Monitoring

- 24/7 SIEM monitoring
- Threat intelligence feeds
- Vulnerability scanning (monthly)
- Dark web monitoring
- Cloud posture monitoring
- Compliance dashboards

Section 06

DFSA Self-Assessment Checklist

✅ Governance & Policy Controls

- □ Board-approved information security policy in place and reviewed annually
- □ Documented roles and responsibilities for cybersecurity functions
- □ Designated CISO or equivalent security officer with direct board access
- □ Regular board reporting on cyber risk and security posture

🔐 Technical Security Controls

- □ Multi-factor authentication enabled for all critical systems
- □ Annual independent penetration testing completed
- □ Network segmentation between production and non-production
- □ Data encryption at rest and in transit using approved standards
- □ Vulnerability management program with defined SLAs
- □ Security monitoring and logging with retention > 12 months

🔄 Business Continuity & Incident Response

- □ Documented and tested business continuity plan
- □ Incident response plan with DFSA notification procedures
- □ Disaster recovery with defined RTO/RPO objectives
- □ Third-party risk management program with due diligence process

Section 07

Why Partner with ITSEC for DFSA Compliance?

🏢 DIFC Expertise

15+ years serving DIFC financial institutions. Deep understanding of DFSA expectations and examination process.

📜 Industry Certifications

CREST, ISO 27001 certified, PCI QSA. Our assessors hold CISSP, CISM, OSCP, and financial services credentials.

💼 Financial Services Focus

Specialized experience with banks, asset managers, exchanges, and FinTech platforms in DIFC.

🤝 Regulatory Relationships

Trusted by regulators and financial institutions across the UAE. Track record of successful DFSA engagements.

60+	100%	15+	24/7
DIFC CLIENTS	COMPLIANCE RATE	YEARS EXPERIENCE	SUPPORT

Start Your DFSA Compliance Journey

Schedule a confidential consultation with our DFSA compliance specialists.
We'll assess your current posture and develop a tailored roadmap.

🌐 www.itsecnow.com 📧 dfsa@itsecnow.com 📞 +971 4 XXX XXXX