INDIALAW

REGULATORY

Regulatory Update: IFSCA Issues Comprehensive Cyber Security & Cyber Resilience Guidelines for MIIs in IFSC (April 2026)

AUTHOR Aditi Rana

PUBLISHED 22 April 2026

Introduction

On April 20, 2026, the International Financial Services Centres Authority ("IFSCA") issued a landmark circular introducing Guidelines on Cyber Security and Cyber Resilience for Market Infrastructure Institutions (MIIs) operating in IFSCs, including GIFT City.

This circular builds upon IFSCA's earlier baseline framework issued on March 10, 2025, and establishes a more prescriptive, risk-sensitive regime tailored specifically for systemically important financial market infrastructure.

Table of contents

Entities Covered

The Guidelines apply to all MIIs operating in IFSCs, including:

- Stock Exchanges
- Clearing Corporations
- Depositories
- Bullion Exchanges

These entities are recognized as systemically critical, given their role in maintaining market integrity, settlement finality, and operational continuity.

Regulatory Objective

The primary objective of the Guidelines is to:

- Strengthen cyber governance and board-level accountability
- Enhance preparedness against evolving threats (including quantum risks)
- Align practices with global standards
- Ensure robust incident detection, response, and recovery

Effective Date

The Guidelines are **effective from April 1, 2026**, with phased compliance timelines prescribed across provisions.

Framework Structure: Seven Cybersecurity Functions

The Guidelines adopt a lifecycle-based approach structured around:

1. Govern
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover
7. Resilience

This aligns with internationally accepted cyber risk management models.

Key Highlights

Governance & Board Accountability

- Mandatory Board-approved Cyber Security Policy
- Formal articulation of risk appetite and tolerance
- Bi-annual oversight by the Standing Committee on Technology (SCOT)
- Appointment of a Chief Information Security Officer (CISO) reporting to the CEO

Notably, cyber security is elevated to a strategic governance issue, not merely an IT function.

Asset Identification & Risk Assessment

- Mandatory enterprise-wide asset inventory, including APIs, cloud systems, and network flows
- Classification of critical assets (including financial data, PII, and internet-facing systems)
- Annual risk assessments, including post-quantum risk evaluation

This ensures visibility across the attack surface, a key regulatory priority.

Strong Preventive Controls (Protect Function)

The Guidelines prescribe granular controls, including:

Access & Identity Management

- Principle of Least Privilege (PoLP)
- Strong authentication and password policies
- Quarterly review of privileged access
- Dual authorization (maker-checker mechanism)

Network & Infrastructure Security

- Defense-in-depth (DiD) architecture
- Network segmentation and isolation
- Deployment of EDR/EPP, firewalls
- DNS filtering and secure gateways

Data Security

- Encryption of data at rest and in motion
- Data Loss Prevention (DLP) across lifecycle
- Cryptographic risk assessments
- Roadmap toward Post-Quantum Cryptography (PQC)

Secure Development & Testing

- Mandatory VAPT (annual / bi-annual for critical systems)
- OWASP-aligned secure development practices
- API security controls

Advanced Detection Capabilities

- Continuous monitoring of logs and network activity
- Implementation of User and Entity Behaviour Analytics (UEBA)
- Real-time anomaly detection and alerting systems

This reflects a shift toward proactive threat hunting and intelligence-driven security.

Incident Response & Reporting Obligations

- Mandatory Cyber Crisis Management Plan (CCMP)
- Incident reporting within 6 hours to IFSCA and CERT-In
- Interim report within 3 days; root cause analysis within 30 days
- Quarterly reporting on cyber-attacks, cyber security incidents and breaches

This introduces strict regulatory timelines, significantly tightening compliance expectations.

Recovery & Business Continuity

- Alignment with Business Continuity Plan (BCP) and Disaster Recovery (DR) norms
- Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Regular backup testing and restoration capability

Cyber Resilience & Testing

- Annual cyber resilience drills and simulations
- Inclusion of critical third-party service providers
- Reporting of lessons learned to IFSCA within 3 months from the end of the financial year

Cyber Security Operations Center (C-SOC)

- Mandatory 24x7x365 Security Operations Center
- Option for shared or standalone SOC models
- Mirror SOC required at Disaster Recovery site

Third-Party & Cloud Risk Management

- Lifecycle-based third-party risk management
- Classification of Critical Service Providers (CSPs)
- Restrictions on subcontracting
- Mandatory cloud security frameworks based on shared responsibility model

Audit & Compliance Requirements

- Annual audit by CERT-In empanelled auditors
- Auditor rotation requirements (3-year cap + cooling-off period)
- Mandatory ISO 27001 certification within 2 years
- CEO/MD declaration of compliance

Enforcement Powers

IFSCA has retained strong supervisory authority, including:

- Power to access IT systems, logs, and infrastructure
- Authority to conduct search and seizure of digital assets
- Oversight extending to third-party service providers

Key Legal & Regulatory Implications

1. Shift Toward Prescriptive Regulation

Unlike the 2025 principles-based framework, this circular introduces granular, enforceable controls, especially for critical institutions.

2. Heightened Board Liability

Cyber risk is now firmly embedded within corporate governance, increasing accountability for directors and senior management.

3. Quantum-Ready Compliance

The explicit inclusion of post-quantum cryptography preparedness signals forward-looking regulation aligned with emerging technological risks.

4. Tightened Incident Reporting Regime

The 6-hour reporting requirement aligns with global best practices and increases regulatory visibility over cyber incidents.

5. Increased Compliance Burden

MIIs must invest significantly in:

- Security infrastructure
- Skilled personnel
- Monitoring and audit systems

Practical Takeaways

- **MIIs**: Must urgently assess gaps and initiate implementation roadmaps
- **Boards**: Need to actively oversee cyber risk governance
- **Legal & Compliance Teams**: Should align internal policies with reporting and audit mandates
- **Technology Teams**: Must prepare for advanced controls, including PQC transition

Conclusion

The April 2026 IFSCA Guidelines mark a major regulatory milestone in India's financial cyber security landscape, especially within IFSCs. By combining governance oversight, technical rigor, and forward-looking risk preparedness, the framework aims to build system-wide cyber resilience.

However, its success will depend on effective implementation, institutional capacity, and continuous regulatory supervision.

For more details, write to us at: contact@indialaw.in

Reference:

[IFSCA-CSD/MSC/2/2026-DCS, April 20, 2026] Guidelines on Cyber Security and Cyber Resilience for Market Infrastructure

Related Practice Areas

Statutory And Regulatory Compliance