waystone | Compliance Solutions

# SEC Operations Paused Amid Government Shutdown: A Strategic Moment for Compliance Readiness

October 22, 2025

Cybersecurity remains a top supervisory priority for the Financial Services Regulatory Authority ("FSRA"). With increasing reliance on digital financial infrastructure, the FSRA has issued enhanced Cyber Risk Management Requirements to promote resilience, operational readiness and regulatory accountability across licensed firms, which will be enforced by 31 January 2026.

Complementing the existing regulatory framework, the FSRA is currently building a Cyber Threat Intelligence ("CTI") Platform that will provide actionable weekly threat intelligence reports, tailored to the financial sector. This initiative is aimed at empowering firms to proactively detect, analyse and mitigate cyber threats through real-time insights, industry collaboration, and centralised information-sharing.

## Key FSRA Cyber Risk Management Requirements

### a) Governance and Oversight

- Boards and Senior Management must assume ultimate responsibility for cyber resilience.
- Firms must maintain clear governance structures, assign accountability to a Chief Information Security Officer or equivalent, and review cyber risks as part of strategic and operational decision-making.
- Regular reporting to the Board on cyber posture, incidents, third-party risks, and remediation activities is expected.

### b) Cyber Risk Framework

- Regulated entities must establish a documented cyber risk management framework aligned with international standards (e.g. NIST, ISO/IEC 27001).
- The framework should cover risk identification, protection, detection, response and recovery.
- Policies and procedures must be periodically reviewed and updated, particularly after significant cyber events or regulatory changes.

### c) Information & Communication Technology ("ICT") Asset Inventory & Classification

- Firms must maintain a comprehensive and continuously updated inventory of all ICT assets, including software, hardware, cloud infrastructure and data repositories.
- Assets must be classified by criticality and sensitivity to ensure proportionate safeguards are applied, especially for systems supporting critical financial services.

### d) Technical Controls

- The FSRA expects firms to deploy layered, defence-in-depth technical controls, including:
  - Multi-factor authentication
  - Network segmentation and firewalls
  - Data loss prevention tools
  - Endpoint detection and response
  - Encryption of data in transit and at rest
- Routine vulnerability scanning, penetration testing and patch management are mandatory to address evolving threats.

### e) Third-Party ICT Risk Management

- Outsourced ICT services, cloud providers and managed security service providers must be subject to due diligence, contractual controls, and ongoing risk monitoring.
- Firms remain responsible for the cybersecurity of outsourced functions and must ensure third parties meet FSRA standards.

### f) Continuous Monitoring and Testing

- Firms must continuously monitor networks, systems and user activity to detect abnormal behaviour.
- Regular cyber resilience testing, including red/purple team exercises and scenario-based threat simulations, must be conducted to assess readiness.

### g) Incident Response Planning

- A robust, documented incident response plan is required, including roles, escalation paths, communication protocols and regulatory notification requirements.
- Significant cyber incidents must be reported to the FSRA promptly.
- Post-incident reviews should be conducted to identify control gaps and prevent recurrence.

### h) Staff Training and Awareness

- Cybersecurity is not solely a technical function; it requires organisational awareness.
- Firms must roll out periodic training for all staff, including phishing simulations and role-specific training for ICT and senior management.

## FSRA CTI Platform – A New Pillar of Cyber Resilience

To support the regulatory strategy, the FSRA is developing a CTI Platform, designed to act as a central hub for sector-specific cyber intelligence.

### Key Features:

### Weekly Actionable CTI Report

- Curated by a dedicated analyst focusing on threats relevant to financial institutions.
- Includes summaries of global and local threat actors, malware trends, phishing campaigns, ransomware alerts and sector-specific vulnerabilities.

### Tailored to the Financial Industry

- Will prioritise intelligence relevant to banks, broker-dealers, asset managers, virtual asset firms and critical financial market infrastructure.

### Free of Charge Service

- All FSRA-regulated entities will gain access without subscription or licensing fees.

## Aggregated from Multiple Trusted Sources:

- **UAE ecosystem:** Cyber Security Council, National Security Operations Centre, national computer emergency response teams
- **Open-source intelligence**
- **Global financial ecosystem feeds**
- **Premium commercial threat feeds**

## Objectives:

- Enhance situational awareness of cyber risks affecting the Abu Dhabi Global Market ("ADGM") and the wider UAE financial community.
- Enable faster detection and mitigation of emerging cyber threats.
- Encourage collaboration between regulators, financial institutions and national security stakeholders.
- Reduce duplication of intelligence efforts and build a centralised knowledge hub.

# Why It Matters for Regulated Firms

The FSRA's enhanced cyber requirements, coupled with the new CTI platform, move ADGM towards a more intelligence-driven, proactive cybersecurity posture. Firms that make effective use of the weekly threat insights will be better positioned to:

- Anticipate attacks before they materialise
- Strengthen technical controls based on real evidence
- Update risk assessments and incident response playbooks
- Inform the Board and senior management with timely, relevant intelligence
- Meet regulatory expectations around continuous monitoring and resilience

# What Next?

As FSRA Authorised Persons work to align their cybersecurity efforts on cyber risk management, building a culture of proactive security is crucial.

At Waystone, our Cybersecurity Team can assist with a range of services, including gap analysis, policy creation, and security awareness training. Contact us today to strengthen your cybersecurity resilience and ensure full regulatory compliance.

**Contact Us** →