waystone | Compliance Solutions

Navigating FSRA IT Risk Management Guidance: A Critical Step Towards Securing Your Organization's Future

July 15, 2025

The Financial Services Regulatory Authority's ('FSRA') Information Technology ('IT') Risk Management Guidance was created to help organizations establish a robust framework for identifying, assessing, and mitigating IT risks.

Technology and data play a fundamental role in driving the decision-making and operations of modern financial institutions. As financial institutions become more reliant on technology, they are increasingly exposed to threats arising from technological vulnerabilities, which can impact their operations and erode customer trust. Recent statistics highlight the growing urgency of implementing strong IT risk management measures. The IBM Cost of a Data Breach Report 2024 indicates that the global average cost of data breaches has risen to US $4.88 million, marking a 10% increase from the previous year and the highest total ever recorded (source: IBM Cost of a Data Breach Report 2024).

Additionally, the report highlights that 1 in 3 breaches involved data that exists outside the centralized and secured data management framework of an organization ("shadow data"), emphasizing the growing difficulty in tracking and safeguarding the ever-expanding volume of data within organizations.

Moreover, organizations that extensively use security AI and automation to prevent breaches save an average of US $2.22 million compared to those that did not.

These figures underline the importance of proactive IT risk management, not only to avoid financial loss but also to safeguard your organization's reputation and preserve customer confidence.

What You Need to Know: Key Areas of the FSRA IT Risk Management Guidance

The FSRA IT Risk Management Guidance covers a wide range of critical areas, from IT strategy alignment with business goals to third-party risk management. Below are some of the most crucial components:

1. Aligning IT Strategy with Business Goals

FSRA emphasizes the importance of aligning IT objectives with broader business goals. Senior management should have the authority, resources, and accountability to execute this strategy effectively. It is essential to ensure that the IT strategy is consistently updated to meet evolving business needs and the growing threat landscape.

Why It's Important:

A lack of alignment between IT and business goals can lead to inefficient resource allocation and missed opportunities. More importantly, it can create significant gaps in your IT risk management approach, leaving your organization exposed to unnecessary vulnerabilities.

2. Establishing Strong Governance for IT Risks

According to FSRA, organizations must designate qualified senior management to oversee IT risk management. The personnel in these roles should possess the necessary skills and expertise to address both current and emerging risks. In addition, a strong competency framework should be established to support ongoing training and development.

Why It's Important:

Without clear accountability and a well-defined governance structure, an organization may struggle to address IT risks in a timely and effective manner. This could result in missed risks or inadequate responses, putting your organization at greater risk of exposure.

3. Third-Party Risk Management

Financial institutions must maintain stringent oversight of third-party vendors, ensuring they comply with your security and risk management standards. The FSRA stresses the importance of regular due diligence, monitoring, and assessing third-party relationships.

Why It's Important:

The increase in supply chain attacks and breaches resulting from third-party vulnerabilities emphasizes the need for diligent third-party risk management. If left unchecked, these relationships can expose your organization to significant security threats.

4. Incident Management and Response

The FSRA IT Risk Management Guidance stresses the importance of having a comprehensive incident management framework. This framework should clearly define roles, responsibilities, and processes for detecting, investigating, responding to, and recovering from IT incidents.

- Why It's Important: Cybersecurity threats are evolving constantly, and no organization is immune. A well-prepared incident management plan can help minimize the impact of potential breaches and ensure business continuity during times of crisis.
- Regulatory Requirements: In addition to having an effective internal incident management strategy, firms must adhere to specific regulatory requirements set forth by the FSRA. According to GEN 8.10.6, firms are required to immediately notify the FSRA of any incidents that impact their operations. This includes incidents such as IT failures and cyber-attacks.
- For IT and cyber incidents, notification is mandatory when there are unscheduled disruptions to online services or business operations. Additionally, any cyber-attack, such as unauthorized intrusions into computer networks, malware infections, or denial-of-service attacks that disrupt or degrade computer functionality and network performance, must be reported promptly.

Failure to comply with these notification requirements can result in regulatory scrutiny, loss of customer data, as well as potential reputational damage for the firm.

5. Cybersecurity and Resilience

In today's cybersecurity landscape, having preventive measures in place is no longer sufficient on its own. The FSRA highlights the need for continuous monitoring, testing, and updates to cybersecurity protocols to ensure they remain effective against emerging threats.

Why It's Important:

A reactive approach to cybersecurity is no longer sufficient. Proactive monitoring and frequent updates to your cybersecurity measures can help protect your organization from the latest threats, minimizing the risk of a breach.

6. Wider Scope

As firms work to build effective IT risk management practices, it is crucial to consider not only the Information Technology Risk Management Guidance but also a range of other regulations and guidance issued by ADGM's authorities. These include key regulations such as the Data Protection Regulations 2021 and the Electronic Transactions Regulations 2021, as well as relevant FSRA rulebooks, including the General Rulebook ('GEN') and activity-specific rules like the Conduct of Business Rulebook ('COBS') and Prudential Rules. Additionally, thematic and technology-focused provide critical insights into managing IT risks effectively in the context of an ever-evolving technological landscape.

7. The Consequences of Non-Compliance: Why Immediate Action Is Needed

The cost of non-compliance with the FSRA's IT Risk Management Guidance can be significant, especially in the event of a cyberattack or IT incident. While the guidance itself is not mandatory, failure to adhere to its best practices can lead to serious regulatory consequences. If a firm experiences an adverse cyber event and has not implemented the required risk management procedures or incident response plans, the FSRA may take regulatory action, including investigations and enforcement measures.

Beyond potential financial penalties, organizations risk reputational damage, loss of customer trust, and heightened scrutiny from regulators. The failure to manage IT risks effectively can expose firms to greater vulnerabilities, especially as cyber incidents continue to rise. Immediate action to align with the FSRA's guidance is critical not only to minimize the impact of such incidents but also to avoid the regulatory fallout and ensure business continuity.

Top 5 Tips for Effective IT Risk Management

To help your organization stay ahead of potential risks, here are five practical tips for managing IT risks effectively:

1. Ensure IT and Business Strategy Alignment: Make sure your IT goals are aligned with your business objectives. This ensures that IT decisions support your broader organizational strategy, reducing the likelihood of missed opportunities and risks.
2. Establish a Strong Governance Framework: Appoint qualified senior management to oversee IT risks and ensure that staff have the necessary training and expertise to manage these risks effectively.
3. Conduct Thorough Third-Party Risk Assessments: Regularly assess your third-party vendors to ensure they meet your security and compliance standards. Supply chain vulnerabilities can often lead to breaches if left unchecked.
4. Develop a Comprehensive Incident Response Plan: Be prepared for the unexpected. Create a well-defined incident management plan (including reporting to the FSRA) and conduct regular tests to ensure that your team can respond quickly and effectively to any incidents.
5. Continuously Monitor and Update Cybersecurity Protocols: As cyber threats are constantly evolving, it is crucial to regularly update your cybersecurity measures and participate in information-sharing initiatives to stay ahead of emerging threats.

Next Steps: Take Action Today

The threat of IT risks is real, and the consequences of ignoring FSRA's IT Risk Management Guidance can be severe. At Waystone, we specialize in helping organizations like yours navigate these complexities.

We can assist you with conducting a gap analysis to assess your current IT risk management framework, review or develop policies and procedures, and provide tailored training programs to upskill your staff. Our team of experts is ready to help you address any gaps in your framework and ensure your organization is fully compliant with FSRA guidelines.

Don’t wait until a breach or incident occurs. Reach out to us today for a consultation and take proactive steps to secure your organization’s future.

Contact us →