FSCA/SARB PA Joint Standard

Ensure your business is COMPLIANT

The new Joint Standard on Cybersecurity and Cyber Resilience requirements has been introduced and you need to be compliant by 1 June 2025

This impacts:

- Small FSP’s, Category I or II
- Medium-sized FSP’s
- Large or digital-first FSP’s

m-konsult.

The FSCA/SARB PA Joint Standard

Background

The **Financial Sector Conduct Authority** (FSCA) and the **South African Reserve Bank** (SARB) have introduced the **Joint Standard on Cybersecurity and Cyber Resilience Requirements**, requiring financial institutions to **achieve compliance by 1 June 2025**.

This new standard is crucial for ensuring that **financial institutions adopt robust cybersecurity measure**s to protect against evolving threats.

Non-compliance could lead to significant regulatory fines and damage to reputations.

What the Join Standard is

The Joint Standard is a comprehensive set of requirements aimed at **strengthening the cybersecurity frameworks of financial institutions**.

It emphasises the **importance of proactive risk management**, **continuous monitoring, and rapid response mechanisms**.

By integrating international best practices with local regulatory requirements, the standard aims to ensure that South African financial institutions are well-prepared to tackle cybersecurity challenges.

m-konsult.

Key Highlights

Key highlights of the Joint Standard include the **implementation of a cyber risk governance and management framework** to identify, assess, and mitigate cyber risks. It also covers cyber threat intelligence management, emphasising the collection and use of cyber threat intelligence to enhance organisational resilience.

Critical Aspects

Other critical aspects include **breach readiness, ensuring effective threat detection and response, employee training and awareness** to bolster readiness against cyber threats, and controls assurance through regular exercises to validate the effectiveness of cybersecurity controls.

The Joint Standard on Cybersecurity and Cyber Resilience Requirements **applies to a wide range of financial institutions**, including **banks** and mutual banks, **insurers, and market infrastructures** such as licensed stock exchanges, central securities depositories, clearing houses, and trade repositories.

It also covers **discretionary Financial Service Providers** (FSPs), Category I FSPs **offering investment fund administration services**, and **administrative** FSPs.

Ensuring you stay compliant

Ensuring you stay **compliant is a necessity** as non-compliance will put your business at risk. Below is a complete **list of the actual compliance requirements** and how to achieve each.

m-konsult.

How to achieve the compliance requirements:

Compliance Requirement	How to Achieve It
Governance and Oversight	Establish a board-approved cybersecurity strategy. Appoint accountable executive(s). Integrate cyber risk into risk management framework.
Cybersecurity Strategy and Framework	Develop and implement a formal, documented cybersecurity framework aligned to standards (e.g., NIST, ISO/IEC 27001).
Information Asset Management	Maintain an updated inventory of information assets. Classify and protect based on sensitivity and criticality.
Risk Identification and Assessment	Conduct regular cyber risk assessments, threat analysis, and impact evaluations. Include third-party risk.
Protection of Information Assets	Apply appropriate security controls: access controls, encryption, endpoint protection, network segmentation.
Identity and Access Management (IAM)	Enforce least privilege access, secure user lifecycle management, and periodic reviews.
Monitoring and Detection	Implement continuous security monitoring, anomaly detection, and threat intelligence integration.
Incident Response Planning and Testing	Develop and test an incident response plan with internal and regulatory notification procedures.

m-konsult.

How to achieve the compliance requirements (cont.):

Compliance Requirement	How to Achieve It
Recovery and Business Continuity	Ensure cyber resilience through tested disaster recovery and business continuity plans.
Logging and Audit Trails	Enable tamper-proof logging with appropriate retention and monitoring policies.
Third-party and Supply Chain Risk Management	Perform due diligence, include cybersecurity clauses in contracts, and monitor vendor risks.
Cybersecurity Awareness and Training	Provide continuous training tailored to roles and responsibilities across the institution.
Independent Reviews and Audits	Conduct annual internal or independent reviews to assess effectiveness of cybersecurity controls.
Regulatory Notification of Material Incidents	Establish protocols to notify FSCA and PA of material cyber incidents within required timeframes.
Reporting to the Board and Senior Management	Deliver regular reports to the board on cybersecurity posture, risks, incidents, and mitigation.
Compliance Deadline	Ensure full compliance with all requirements by 1 June 2025.

m-konsult.

The risk to the business and its officers of non-compliance is as follows:

Category	Implication	Description
Regulatory	Enforcemenet Action	FSCA and PA may impose sanctions, penalties, or mandate corrective actions.
Regulatory	License Risk	Persistent non-compliance could lead to suspension or revocation of FSP license.
Regulatory	Reporting Breach	Failure to report incidents may be treated as a breach of regulatory obligations.
Operational	Cyber Incidents	Increased risk of cyberattacks, ransomware, and data breaches due to weak controls.
Operational	Business Disruption	Unpreparedness may cause prolonged outages and financial losses during incidents.
Legal	POPIA Violations	Breaches of personal data can trigger fines or enforcement under South Africa's POPIA.
Legal	Third-Party Liability	Clients or partners may pursue legal claims for losses from preventable cyber incidents.
Legal	Insurance Rejection	Cyber insurance claims may be denied due to non-compliance with security standards.
Reputational	Client Trust Erosion	Customers may lose trust in the institution, leading to churn and revenue loss.
Reputational	Investor Confidence	Non-compliance could reduce confidence among investors and stakeholders.

Ready to Comply?

Let’s Chat.

Book a 30-min discovery session.

Contact Us

Marius.burger@m-konsult.com

+27 82 901 6979

www.m-konsult.com

m-konsult.