SMBsecure™ FSP ComplianceSuite

50+ Controls Checked For Your Cyber Joint Standards Compliance.

Reduce COST

Reduce. COMPLEXITY

Improve COMPLIANCE

FSP VALUE

Great Value Cybersecurity Compliance

> 50+ Controls Checked + Dark Web Monitoring.
> 7 Pillars of JS02 Addressed.
> NIST/ISO/CIS CSF Compliance Assessments.
> R1M Cyber Warranty.

> **Joint Standard Toolkit.**

BONUS:

+ Live AI Assistant & Compliance Tracker.
+ FREE Policy Templates.

What Is The FSCA Cyber Joint Standard Regulations?

The twin peaks regulators of the South African financial industry, the Financial Sector Conduct Authority (**FSCA**) and the Prudential Authority (**PA**), have introduced two pivotal sets of regulations: Joint Standard 1 of 2023 on IT Governance and Risk Management (**JS01-2023**) and Joint Standard 2 of 2024 on Cybersecurity and Cyber Resilience Requirements (**JS02-2024**). These standards, collectively referred to as the "**cyber joint standards**", establish a comprehensive framework for how financial institutions must manage their technology and cybersecurity risks. These framework regulations are significant to bolster the resilience of South Africa's financial services industry against mounting cyber threats.

Why You Need To Comply With The Cyber Joint Standards?

In the current landscape of ever-present and evolving digital threats, attacks and scams, it is crucial for a FSP to comply with the Cyber Joint Standards. Compliance is not merely a regulatory burden; it is a fundamental aspect of responsible business practice. Complying with the Cyber Joint Standards is essential for protecting your clients, your own FSP business, and the stability of the financial system. The FSCA and the PA have been empowered by the Financial Sector Regulation Act to set these standards. Non-compliance can lead to severe penalties, including **Substantial Fines**: The regulators have the authority to levy significant financial penalties for breaches of the Joint Standards. **Enforcement Action:** This can range from mandated remedial actions to, in severe cases, the **suspension or revocation of an FSP's license to operate**.

How To Comply With The Cyber Joint Standards?

As an FSP you must embed resilience and security into your business culture, driven from the executive level down. This means treating compliance not as an IT project, but as a core, ongoing business function focused on governing, managing risk and **building genuine resilience**.

How SMBsecure™ Helps You Comply With JS01 & JS02?

SMBsecure™ simplifies and enhances cybersecurity for small and mid-sized FSPs, helping to meet several key requirements of the FSCA Joint Standards. It inexpensively offers broad coverage for compliance that includes data protection, risk management, external & internal attack surface monitoring, vital controls, reporting and assessments, and employee training. **ComplianceKate®** is your personal AI Assistant to guide you through everything. It's all backed with a Cyber Warranty to provide remediation & financial peace-of-mind. This all leads to **lower risk**, **improved compliance**, **increased business resilience** and **Trust**.

Cost Effective, All-in-One Cybersecurity Compliance

Hi, I'm Kate. Your AI Assistant here to help you with questions, scenarios, policies, templates and guidance related to Joint Standards 1 & 2, POPIA, PAIA, Frameworks and SMBsecure™ info.

SMBsecure™ | FSP ComplianceSuite

www.smbsecure.co.za

www.compliancesuite.co.za

Get Data Security & Compliance
as part of your everyday data processing…

HOW IT WORKS

The ultra affordable **SMBsecure™** CompliianceSuiite leverages patented technologies from leading and world class technology vendors that can be deployed in minutes to address cybersecurity compliance and make securing data on PCs, Macs, USBs, Mobiles and Emails a **Total Breeze.**

The Financial Services Industry Is Built On Trust

Clients entrust you with their sensitive personal and financial information, as well as their hard-earned money. A successful cyberattack can lead to the theft of this data and these funds, identity theft, significant financial loss and emotional distress to consumers. **SMBsecure™** ensures that your small FSP business will have robust security measures in place to protect client information from unauthorised access & disclosure.

A Cyber Incident Can Be Costly For Your FSP Business

The consequences can include:

> **Financial Loss:** The direct costs of a breach can be enormous, encompassing the theft of funds, the expense of remediation, regulatory fines, and legal fees.

> **Reputational Damage:** The loss of client trust following a cyberattack can be difficult. This can lead to a mass exodus of clients and a severely tarnished brand.

> **Operational Disruption:** A successful attack, such as a ransomware incident, can bring business operations to a complete standstill, preventing your FSP business from serving its clients and conducting its business.

	ComplianceSuite
Full Device Encryption	✓
Remote Lock / Kill / Locate	✓
RiskResponders® for Automatic & Off-Network Protections + MFA	✓
Access Controls, USB Port Blocking & M365/Google MFA Analysis	✓
*Secure PDF Email Encryption + Check4Phish™	✓
SendGuard365 Lite for Users to confirm recipients when emailing	✓
Cybersecurity Awareness Training + Dark Web Monitoring	✓
Vulnerability Assessments & Attack Surface Monitoring	✓
Joint Standard Compliance Toolkit + ComplianceKate® AI Assistant	✓
ComplianceEZ® for NIST / CIS / ISO27001 CSF Assessments	✓
Managed DMARC & MTA-STS for Email Security Compliance	✓
**R1M Cyber Warranty	✓

Encrypt | **Safeguard** | **Protect** | **Defend**

* COM Addin for Microsoft Classic Outlook on Windows PC. ** Cyber Warranty only applies to FSPs domiciled in South Africa.

SMBsecure™

SMBsecure™

Your Quick Guide to Cyber Joint Standard 2 Compliance.

Joint Standard 2

is a mandatory framework from South Africa's **FSCA** and **PA**, setting minimum requirements for cybersecurity and resilience in the financial sector. It moves beyond traditional IT security to demand a holistic, board-led approach to managing cyber risk, ensuring the stability and integrity of financial systems.

A Critical Mandate: Incident Reporting

One of the most stringent requirements is the notification of material cyber incidents to the authorities.

24 Hours > Maximum timeframe to report a material cyber incident to the FSCA/PA.

JS2 doesn't exist in a vacuum. It complements existing local regulations like POPIA and aligns with international best practices.

The Shift to Holistic Resilience

JS2 redefines cybersecurity as a core business function, not just a technical task. The goal is to ensure operational continuity and protect the entire financial ecosystem.

The 9 Pillars of Joint Standard 2 Compliance

Achieving compliance requires a structured approach across nine fundamental domains. Each pillar represents a critical area of focus, from high-level governance to on-the-ground technical controls and continuous testing.

Governance & Board Accountability
Establish clear board-level ownership and a dedicated sponsor. Define and assign cybersecurity roles and ensure the board oversees and approves the entire framework.

Cybersecurity Strategy & Framework
Develop a formal, documented strategy aligned with your risk appetite. This is a living document that must be regularly reviewed and updated to counter evolving threats.

Risk Management & Assessment
Conduct ongoing risk assessments to identify threats. Maintain a critical asset inventory to prioritize protection and manage the swift remediation of all identified vulnerabilities.

Cybersecurity Fundamentals
Implement essential technical controls: robust Identity and Access Control with MFA, password hygiene, data encryption, device-lock, secure system configurations, and network protection.

Incident Detection & Response
Deploy real-time detection systems. Develop and regularly test a comprehensive incident response plan, including data backup strategies for rapid recovery.

Third-Party Risk Management
Extend your cybersecurity standards to all vendors. Align contracts and SLAs with JS2 obligations, as accountability cannot be outsourced.

Training & Awareness
Implement regular, comprehensive cybersecurity training for all staff, from the front desk to the boardroom, to build a strong **Human Firewall**.

Testing & Continuous Improvement
Regularly test all controls through vulnerability assessments, penetration testing, and simulations. Use findings to adapt and improve your resilience capability.

Compliance & Documentation
Maintain meticulous documentation for everything: risk assessments, test results, training records, and policies. Be ready to prove compliance to regulators.

Your Path to Compliance

Achieving compliance is a journey, not a destination. Follow this structured, phased approach to build and maintain a robust and resilient cybersecurity posture in line with JS2's requirements.

1 Gap Analysis
Assess your current state against JS2 requirements to identify shortfalls and prioritize actions.

→

2 Strategic Implementation
Remediate gaps by updating policies, implementing controls, and training personnel.

→

3 Continuous Improvement
Establish a cycle of testing, monitoring, and adapting to ensure ongoing resilience and compliance.

SMBsecure™ | FSP ComplianceSuite
www.smbsecure.co.za
www.compliancesuite.co.za

Go Beyond Compliance

Embracing JS2 is more than a regulatory hurdle; it's an investment in trust, operational resilience, and competitive advantage. A strong cybersecurity posture and audit-readiness is the foundation of a modern FSP.