Navigating regulatory waves:

Strengthening cybersecurity in the evolving financial landscape

Introduction to the three new interrelated regulations for the financial sector

As financial sectors integrate advanced technologies and grow more reliant on interconnected ecosystems, we are seeing escalating cyber threats and attacks.

In response to the digital acceleration and evolving threat landscape, the South African Reserve Bank (SARB) and Financial Services Conduct Authority (FSCA) have released a series of regulations aimed at ensuring that the financial sector is able to embrace the opportunities presented by these new technologies in a way that is safe, responsible and resilient to the evolving cyber threat landscape.

Three interrelated regulations

Two ‘joint standards’ were released in collaboration between the SARB’s Prudential Authority and the FSCA. In addition to these two ‘joint standards,’ the SARB issued an additional regulation specifically to protect the National Payment System (NPS):

Key information

	Joint Standard 1: IT Governance and Risk Management	**Joint Standard 2:** Cybersecurity and Cyber Resilience	**Directive:** Cybersecurity and Cyber Resilience
Published	15 November 2023	17 May 2024	17 May 2024
Commences	15 November 2024	1 June 2025	17 August 2024
Applies to	Financial institutions	Financial institutions	Payment institutions

Crucial requirements

There are 5 crucial requirements contained in the new regulations that institutions need to be aware of in addition to their best practice standards:

1. **Board level accountability**
The regulations require that the board takes accountability for embedding good IT governance and cyber resilience practices into the daily operations and culture of the organisation.

2. **Demonstrate compliance**
Institutions need to report on a regular basis (at least annually) that they have reviewed, tested and improved their systems and processes.

3. **Independent assurance**
The regulations require that institutions obtain independent assurance (e.g. internal audit or an external assurance provider) to prove that the institution is compliant with the requirements.

4. **End-to-end ecosystem**
The regulations require that institutions demonstrate that their full ecosystem is in compliance with the requirements.

5. **Risk-based approach**
This risk-based approach is premised on the principle that institutions need to identify and risk assess all their technology, data and processes.

Businesses can navigate new regulations effectively and ensure sustainable compliance by using a comprehensive approach.

This includes pre-assessments, self-assessment tools, board awareness programmes, policy updates, and independent assurance services.

This strategy helps organisations and their stakeholders meet regulatory requirements with confidence.

Practical steps

It is important that institutions see the regulations as an opportunity to review and enhance its existing practices and capabilities as it navigates the evolving digital and threat landscape.

We recommend 5 practical steps:

Board positioning and awareness
Ensure that the board understands the requirements and its responsibilities. The tone from the top is important in building a culture of good governance and resilience.

Discovery and prioritisation
Start with the discovery and prioritisation processes to ensure that you have a complete understanding of your critical assets and processes (including at suppliers and ecosystem partners) as well as to ensure that your controls are commensurate with the risk.

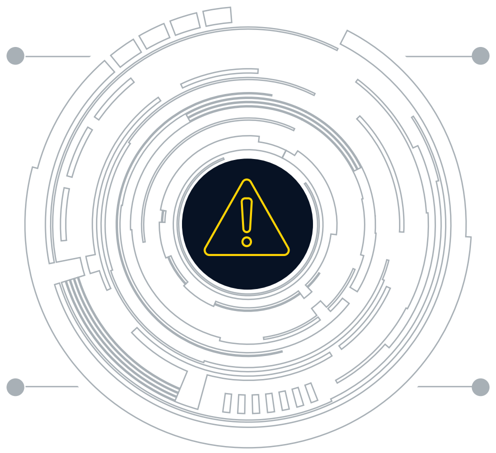
Refresh practices and policies
Approach the three regulations holistically by refreshing existing policies and procedures to include any additional requirements or to enhance or change any systems and processes. In addition, overlay the requirements into an existing control framework (or create one if you don't have an existing control framework) in order to demonstrate compliance.

Roles and responsibilities across ecosystem
It is vital that all stakeholders understand their roles and responsibilities in executing the requirements as well as in being able to demonstrate compliance. This includes stakeholders across the ecosystem and throughout the organisation.

Continuous visibility
Compliance to the regulations is not a once-off exercise. To be effective and add value on a continuous basis, it is important to build a mechanism to have ongoing visibility regarding the organisation's posture and compliance status. This could be through dashboards providing a 'single pane of glass' to management and the board.

Pitfalls

As organisations navigate the new regulations, there are common pitfalls to avoid.



Forgetting about the full ecosystem
Ignoring the entire ecosystem approach means that even the most robust and effective controls within the organisation may still not result in compliance.

Tick box approach to compliance
Institutions should consider the standards as an opportunity to ensure that IT governance and cybersecurity practices are prioritised, risk-based, aligned to best practices and embedded throughout the ecosystem.

One-size-fits-all approach
Taking a one-size-fits-all approach means that organisations may be over-controlling certain areas while not applying sufficient safeguards in others.

Relying on existing frameworks and self-assessments
Building a portfolio of evidence to demonstrate compliance can take time. It is important to start early and build the collection of evidence into the processes.

Once off exercise to appease regulatory bodies
Approaching the regulations as a once-off exercise, will not add value or result in meaningful improvements.

How EY can help

Pre-assessment
Assess your readiness for the regulations and craft practical steps for addressing any compliance gaps

Framework and self assessment tool
Consolidated framework containing all regulations as well as industry standards to help you assess your compliance in an efficient way on a regular basis

Board awareness
Board education and awareness to ensure that they understand, in business terms, the importance of the regulations as well as how to practically discharge their roles and responsibilities

Refresh policies and procedures
Enhance and update existing policies, systems and processes to accommodate the new regulations, including embedding in sustainable ways of working

Independent assurance
Conducting independent tests to demonstrate compliance in line with the requirements of the regulations

3rd party assurance
Understand the full ecosystem and ensure that all stakeholders are compliant

Contacts

Candice Wilson
Cyber Leader
E: Candice.Wilson@za.ey.com
M: +27 82 410 0767

Lutfiyyah Ahmed
Senior Manager: Cyber
E: lutfiyyah.ahmed@za.ey.com
M: +27 82 082 6056