

Law Navigator



Helen Littlewood
SURF Head of Product

Cybersecurity and Cyber Resilience

This edition of Law Navigator focuses on Joint Standard 2 of 2024: Cybersecurity and Cyber Resilience Requirements, issued by the Financial Sector Conduct Authority and the Prudential Authority on 17 May 2024 and effective from 1 June 2025. This is not intended to be a summary of the Joint Standard but addresses specific aspects thereof.

Aim

The Joint Standard aims to strengthen the management of cybersecurity risk in a manner that will ensure consistency across different financial institutions, thereby enhancing the protection of financial customers and improving the overall resilience of the financial services ecosystem.

The Joint Standard is drafted in an outcomes and principles-based manner and sets out general and overarching principles. It outlines the minimum requirements and standards to be implemented by the regulated financial institutions in light of their highly digitalised operations. The impact on a financial institution when a cyber incident occurs is significant, both with regards to the financial soundness of the institution and to its customers.

The extent of the resources necessary to implement the requirements of the Joint Standard and the assessment of a financial institution's compliance will depend on the nature, size, complexity and risk profile of the financial institution; larger financial institutions may thus have to implement additional measures to meet their actual risks. When conducting supervisory reviews, the authorities may assess controls and processes in respect of the nature, size, complexity and risk profile of the financial institution.

The main aims of the Joint Standard are to:

- Ensure that financial institutions establish sound and robust processes for managing cyber risks;
- Promote the adoption of cybersecurity fundamentals and hygiene practices to preserve the confidentiality, integrity and availability of data and IT systems;

- Ensure that financial institutions undertake systematic testing and assurances regarding the effectiveness of their security controls;
- Ensure that financial institutions establish and maintain cyber resilience capability to be adequately prepared to deal with cyber threats; and
- Provide for notification of material cyber incidents by the regulated entities to the authorities.

Cybersecurity and cyber resilience

The case of State v Lucky Majandile Erasmus is an example of how the collaboration between all stakeholders within with the framework of the Cyber Crimes Act can assist in the fight against cyber-crime.

Lucky Majandile Erasmus, a former employee of Ecentric Payment Systems, illegally installed software on his previous company's IT systems to enable remote access and then attempted to extort money from his previous company by threatening to publish data across various platforms.

Applying this case to the Standard and to retirement funds, Erasmus can be classified as a cyber threat. Cybersecurity means protecting the fund's systems from this kind of attack. The case shows how imperative it is for a fund to have strong security and to keep a look out for risks from inside the fund and/or its administrator. Instead of giving in to the ransom demands, Ecentric worked with the police and cyber experts to deal with their cyber breach. This is an example of cyber resilience; having a plan to deal with a cyber threat. Erasmus was eventually convicted on 17 charges under the Cyber Crimes Act and will serve five years direct imprisonment. The case highlights how attitudes to cyber security have changed and improved:

Prior to the case:

- Companies tended to underestimate insider threats.
- As the Cyber Crimes Act was new, there was little to no precedent and accordingly the laws were rarely tested.
- Companies feared public knowledge of cyber-attacks and were quick to pay off ransom requests to make the problem go away.

After the case:

- Companies are more informed and are likely to be more cautious of insider threats.
- Those that do not follow the requirements of the Cyber Crimes Act will be sentenced in a court of law.
- Teamwork with stakeholders to combat cyber-attacks must be widely embraced.

Regulated financial institutions

The Joint Standard applies to financial institutions that, due to their role within the financial ecosystem, are highly vulnerable to cyber threats. Such entities include:

- A discretionary financial services provider (FSP) as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003 – **an FSP performing intermediary services with discretion to choose a specific financial product for their client**;
- A category I FSP that **provides investment fund administration services**, as contemplated in section 3(a) of the Determination of Fit and Proper Requirements for Financial Services Providers, 2017;
- **An administrative FSP** as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003;
- **A pension fund** licensed under the Pension Funds Act; and
- **A pension fund administrator** approved in terms of section 13B of the Pension Funds Act.

The Joint Standard does not at this stage apply to brokers, nor does it impose an obligation on insurers to ensure that brokers have adequate cyber risk and cyber resilience policies.

Third parties

The Joint Standard does not apply directly to third-party service providers. Any entity that is not the financial institution or part of the group to which the financial institution belongs qualifies as a third party.

Where a financial institution outsources certain functions to a third party or otherwise utilises a third party's services, it does not relieve the financial institution of its responsibilities under the Joint Standard. The financial institution remains ultimately accountable for complying with the requirements in the Joint Standard. It must ensure that the controls of the third party are equivalent or similar to those required in terms of the Joint Standard. The third-party service provider must have the operational ability to protect the financial institution's data, which includes the necessary cybersecurity and cyber resilience frameworks. The financial institution must ensure that roles and responsibilities are clearly defined in the contract or service level agreement entered into with that third party.

Devices

Paragraph 6.5 of the Joint Standard requires that a financial institution must establish cybersecurity policies, standards, processes and procedures that are informed by industry standards and best practices to manage cyber risks and safeguard IT systems and information assets.

An information asset is defined as any piece of data, device or other component of the environment that supports information-related activities. In the context of this Joint Standard, information assets include IT assets and exclude paper-based information. Cloud data is part of information assets and should be treated the same as data on site.

Each device with access to a financial institution's network should be configured with the financial institution's minimum-security standards; this includes mobile devices authorised to access the financial institution's systems. The financial institution must implement appropriate measures to prevent and detect unauthorised access to its data and its modification, copying or transmission, as well as data theft in systems and endpoint devices. To that end it must ensure that all devices used are encrypted, taking into account the financial institution's nature, scale, complexity and risk profile. Where a financial institution's employees or other persons with access to its

data use their own devices (referred to as Bring Your Own Device), the financial institution must ensure that only authorised devices with security configurations similar to those of the financial institution are used.

Retirement fund

The definition of financial institution in the Joint Standard includes retirement funds, which must comply with the requirements as set out in the Joint Standard.

The fund must establish and maintain a cybersecurity strategy that is approved by its board of trustees and review this strategy regularly (at least annually) to address changes in the cyber threat landscape, allocate resources, identify and remediate gaps and incorporate lessons learnt, as required in paragraphs 6.1 and 6.2 of the Joint Standard.

Due to the nature of the risk related to cybersecurity and cyber resilience, it is imperative that the review is conducted at least once a year by an independent function such as risk, compliance, internal audit or an external auditor. The purpose of the review is to ensure the adequacy and effectiveness of the framework.

The fund must implement appropriate and effective cyber resilience capabilities and cybersecurity practices to prevent, limit and/or contain the impact of a potential cyber event or cyber incident as required in paragraph 7.2.1 of the Joint Standard.

A retirement fund must ensure that when it shares sensitive data, it does so in the most secure manner and in consideration of applicable legislation and the Joint Standard.

If a material cyber incident or information security compromise occurs, the fund must notify the responsible authority thereof. Where the fund's members are affected, the fund must communicate this to the affected members and inform them of the possible consequence within 24 hours of the incident or compromise occurring.

Paragraph 7.6.2(iii) of the Joint Standard requires that a retirement fund:

Participate in cyber threat information-sharing arrangements with trusted external parties to –

- (a) share reliable, actionable cybersecurity information regarding threats, vulnerabilities, and incidents to enhance defences; and*
- (b) receive timely and actionable cyber threat information.*

This does not mean that the fund must share specific or member-specific information; the modus operandi, trends, lessons, indicators of compromise and challenges will form part of the information-sharing arrangements.

The fund must notify the responsible authority of any material cyber incident or information security compromise.

Conclusion

The Joint Standard should lead to the enhanced protection of the data of retirement fund members and of the clients of other financial institutions. However, such individuals remain vulnerable to cyber threats in their personal capacity and should take necessary precautions to ensure they do not fall victim to data theft. Financial advisors and employers can play a vital role in educating fund members about individual responsibility for safeguarding personal data.