AON

The Aon Decoder

July 2025 | Edition 181

Contents

Legal & industry update – July 2025

In this publication we look at:

- FSCA Communication 12 of 2025 (General): Update on the roll-out and implementation of the cross-sectoral Conduct of Business Return (OMNI-CBR) for financial institutions
- Joint Standard 2 of 2024: Cybersecurity and resilience – ongoing requirements from retirement funds

FSCA Communication 12 of 2025 (General): Update on the roll-out and implementation of the cross-sectoral Conduct of Business Return (OMNI-CBR) for financial institutions

The FSCA's Omni-CBR is a cross-sectoral Conduct of Business Return designed to facilitate streamlined, quarterly reporting by financial institutions to provide the FSCA with reliable, comparable conduct information to monitor and ensure fair customer outcomes in the financial sector. Initially released for comment on 30 October 2020, the OMNI-CBR has been through a robust consultation process and in July 2022, the FSCA published a roadmap to its implementation. The final version of the OMNI-CBR, or at least commentary from the FSCA on its progress, was expected in July 2024.

On 11 June 2025 the FSCA issued Communication 12 of 2025 where it confirmed that during the previous 18 months, the FSCA had accelerated several strategic re-prioritisation and organisational transformation efforts. These efforts were geared towards refining the FSCA's focus and significantly improving its operational efficiency and effectiveness.

The FSCA needs to modernise its regulatory capabilities if it is to deliver on its three-year regulatory strategy. Thus, the FSCA has adopted a multi-year organisation wide Digital Transformation Strategy, which includes major investments in new and enhanced technology. The most notable has been the procurement of a supervisory technology (SupTech) platform, namely the Integrated Regulatory Solution (IRS). It is expected that this will significantly improve how the FSCA engages with financial institutions in the future.

The conceptualisation and development of the OMNI-CBR pre-dated the roll-out of the FSCA's Digital Transformation Strategy and the procurement of the IRS. To a certain extent, previous iterations of the OMNI-CBR attempted to achieve similar objectives to the IRS, but were designed for a largely manual, less modernised supervisory environment.

Implementing the IRS has provided the FSCA with an invaluable opportunity to re-think the supervisory data collection model initially contemplated under the OMNI-CBR and instead explore a more streamlined, intuitive and incremental approach leveraging the new technological capabilities being introduced through the SupTech platform.

Because of this, the FSCA has confirmed that financial institutions are not expected to initiate or progress any internal OMNI-CBR related initiatives or system development and implementation efforts until further communication is issued on the roll-out of the IRS.

Joint Standard 2 of 2024: Cybersecurity and Resilience (JS 2 of 2024) - ongoing requirements from retirement funds

Although Joint Standard (JS) 2 of 2024 took effect on 1 June 2025, ongoing compliance requires continued efforts beyond the implementation date. JS 2 of 2024 outlines specific obligations for financial institutions, like retirement funds, to make sure they stay compliant with cybersecurity and cyber resilience standards. It goes to great lengths to set out detailed roles and responsibilities to safeguard members from potential cyber threats, attacks and/or breaches.

Summarised below are trustees' ongoing responsibilities:

1. Review the fund's cybersecurity strategy

The fund's cybersecurity strategy must be reviewed at least annually to:

- address changes in the cyber threat landscape,
- incorporate cyber risk management into the fund's governance structures with independent oversight, and
- ensure that it remains aligned with the fund's other policies and other applicable laws (for example, the Protection of Personal Information Act).

2. Update policies, processes and controls

The fund's cybersecurity policies, standards, processes and procedures must be continuously updated to reflect evolving risks, updates in technology and increased sophistication of cyber threats, including the ability to recover from cyber events.

3. Conduct regular testing and assurance

Financial institutions must undertake systematic testing, ongoing monitoring and validation of their cybersecurity measures to evaluate the effectiveness of their security protocols - including regular penetration testing, vulnerability assessments and other cybersecurity exercises to identify and address weaknesses.

4. Incident management and reporting

Retirement funds must maintain effective detection and response capabilities, including the ability to manage and mitigate cyber incidents. Funds are required to notify the FSCA or Prudential Authority of material cyber incidents within 24 hours, using the prescribed template.

5. Ongoing training and awareness

Ongoing trustee training is mandatory to make sure trustees remain abreast of evolving cyber risks and incidents. Training programmes must be relevant in the rapidly changing fintech landscape.

6. Governance and oversight

Ongoing reporting is required to ensure that the trustees, or a relevant sub-committee, are kept meaningfully informed of the fund's cyber security and resilience position.

7. Third-party risk management

Funds must conduct ongoing monitoring of third-party service providers to manage supply chain vulnerabilities. This includes maintaining an inventory of critical service providers and ensuring business continuity plans are in place.

8. Continuous improvement

The regulators expect retirement funds to continuously improve their cybersecurity and cyber resilience practices, adapting to new threats and regulatory guidance. This includes integrating lessons learned from incidents, either their own or incidents in the wider industry.

Remember, your retirement fund is a financial institution as defined and runs the risk of incurring administrative penalties if it does not comply with JS 2 of 2024. Your fund administrators are referenced separately and they must also comply with JS 2 of 2024. The FSCA has specifically noted that retirement funds cannot simply rely on their administrator's cybersecurity controls alone.

This publication does not provide advice or legal opinion. If you have any questions/comments on the above, please contact your consultant.

Aon South Africa (Pty) Ltd, Actuarial, Healthcare & Retirement Fund Consultants
The Place, 1 Sandton Drive, Sandhurst, Sandton, 2196
P O Box 78367, Sandton, 2146
+27 11 944 7000 | www.aon.co.za