VERBATIM

November 2026

ISSUE 134



LEGAL & INDUSTRY UPDATE – NOVEMBER 2026

In this publication we look at:

- Feedback from the recent FSCA webinar to the retirement fund industry on: Understanding Joint Standard 2 of 2024 - Cybersecurity and Cyber Resilience Requirements (the JS)

CYBERSECURITY GOVERNANCE: FSCA CLARIFIES EXPECTATIONS FOR RETIREMENT FUNDS

The Financial Sector Conduct Authority's (FSCA) webinar on 27 October 2026 reinforced a clear message: retirement funds may outsource operational functions, but not accountability. Presented by Andile Mjadu of the Regulatory Frameworks Department, the session explored what Joint Standard 2 of 2024 means in practice, particularly for board oversight, service provider assurance and incident preparedness.

For trustees, the challenge is to turn policies into effective governance. The sections below draw together the webinar's practical guidance and the Joint Standard's requirements. Where appropriate, the relevant paragraphs from the Joint Standard are included to situate the webinar's content and give further context.

BOARD RESPONSIBILITY REMAINS PARAMOUNT

Paragraph 4.1 of the JS places ultimate responsibility for compliance and cyber risk oversight on the governing body. A committee may take on primary oversight activities, but the board remains accountable. Paragraph 4.2.3 of the JS also requires security responsibilities to be clearly defined in third party contracts or service level agreements.

This applies even where a fund has no systems of its own. Trustees must question the arrangements supporting the fund, rather than leave cybersecurity entirely to the administrator. Paragraph 5 reinforces the need for clear responsibilities, integration into governance structures and separation of duties to avoid conflicts.

Practical action: Table a cybersecurity responsibility matrix identifying operational owners, oversight responsibilities and escalation routes, including those involving service providers.

STRATEGY MUST TRANSLATE INTO EFFECTIVE CONTROLS

The JS requires a board approved cybersecurity strategy and framework. The strategy must be reviewed at least annually, while the framework requires an independent review for adequacy and effectiveness at least annually. These are separate obligations.

The webinar stressed that policies must work in practice. Core controls include identity and access management, data loss prevention, **least-privilege access** and auditable activity records.

Least-privilege access is a cybersecurity concept requiring that human users, system accounts, applications, and automated processes receive only the minimum level of access rights necessary to perform their specific job functions, and nothing more.

VERSO®
EMPLOYEE BENEFITS CONSULTING (PTY) LTD

Tel: 087 330 2001
E-mail: info@verso.co.za | Web: www.verso.co.za
An authorized Financial Services Provider. License number 53857

Paragraph 8.3 of the JS requires multi-factor authentication (MFA) for critical system functions and internet access to applications containing sensitive information. Administrative and privileged accounts require MFA or, at minimum, privileged access management mechanisms. Simply confirming that a provider has an MFA policy is not enough.

Practical action: Request a compliance report covering strategy approval, the latest independent framework review, evidence of key controls and outstanding remedial actions.

Outsourcing requires meaningful assurance

The webinar encouraged measurable contractual incident notification timelines, rather than clauses merely requiring notification. Funds should negotiate audit or independent assurance rights where possible and consider concentration risk.

Paragraph 7.2.3 of the JS requires appropriate protection for information assets managed by third parties. Where a fund relies on a provider's control testing, paragraph 7.7.1 requires it to be satisfied that the testing's nature and frequency match the relevant risks.

The webinar did not prescribe a particular assurance certification or expressly endorse provider-issued cyber assurance letters as sufficient on their own. A letter of comfort therefore needs scrutiny of its scope and supporting verification.

Practical action: Review critical provider agreements alongside assurance reports, checking notification timelines, access to independent evidence and unresolved findings.

INCIDENT RESPONSE INCLUDES MEMBER COMMUNICATION

Following an incident, funds should establish which systems are affected, who depends on them and how extensive the disruption is. The webinar also stressed early, concise member communication in plain language, even before all details are available.

Paragraphs 7.4 and 7.5 of the JS require response and recovery capabilities, customer communication arrangements and an incident management plan. Recovery arrangements must align with objectives for acceptable data loss and the time within which systems should be restored.

Regulatory notification is separate. Paragraph 9.1 requires notification to the responsible authority, in the prescribed form and manner, after an incident or compromise is classified as material.

Practical action: Approve a protocol identifying who assesses materiality, authorises member communications and submits regulatory notifications.

TESTING MUST LEAD TO ACTION

Although the webinar account described simulations and tabletop exercises as strongly encouraged, paragraph 7.7.4 of the JS requires regular scenario-based simulations, including adversarial attack and defence simulation. A **tabletop discussion** should not automatically be treated as meeting that wider requirement.

A cybersecurity **tabletop exercise (TTX)** is a discussion-based, non-technical simulation where key stakeholders walk through a hypothetical cyber incident, such as a ransomware attack, data breach or insider threat, in a low stress, controlled environment.

Paragraph 7.7.1 requires time bound remediation plans and board escalation of deficiencies that cannot be remedied promptly. Paragraph 7.2.7 separately requires governing body training.

Implementation must reflect the fund's nature, size, complexity and risk profile. Proportionality does not remove these responsibilities.

Practical action: Schedule a simulation with critical providers and require a remediation plan with named owners and deadlines.

Cybersecurity compliance must be demonstrated, not merely documented. Boards need to show that they understand the risks, challenge assurances and have tested how their arrangements will work when an incident occurs.

Practical action – a checklist to guide your thinking and strategy

FOR THE FUND

1. Committee mandate / Terms of Reference covering cyber risk.
2. Governance framework / RACI showing cybersecurity roles and responsibilities.
3. Risk management framework extract showing cyber risk inclusion.
4. Training records / attendance register for board cyber awareness training.
5. Sample SLA / contract extract showing cybersecurity responsibilities of service providers.
6. Approved cybersecurity strategy document.
7. Evidence of annual strategy review (board minutes or review report).
8. Latest independent review report.
9. Latest security risk assessment report.
10. Incident Response Plan including member cyber incident communication plan or procedure.

FOR EACH OF THE FUND'S SERVICE PROVIDERS

In addition to the documents required for the Fund above:

1. Access control policy.
2. Evidence of access review.
3. Data loss prevention policy.
4. Service provider security requirements in SLA / contract.
5. Backup and recovery policy.
6. Evidence of backup testing.
7. Business continuity / disaster recovery plan extract showing RTO and RPO.
8. Cyber incident response plan.
9. Evidence of testing of the incident response plan (e.g. simulation exercise report).
10. Incident report and FSCA notification (if applicable).
11. Latest vulnerability assessment report.
12. Latest penetration testing report.
13. Latest cyber simulation exercise report.
14. Remediation register / tracking log.
15. Patch management policy.
16. Evidence of patch application.
17. Third-party security assurance reports (e.g. SOC 2 reports or audit reports from the administrator).
18. Material incident classification criteria / procedure.
19. Copies of any FSCA notifications submitted during the reporting period.
20. Two-pot fraud risk assessment.
21. Identity verification controls documentation.