Trustee Tutor 22:
IT governance and cybersecurity

Retirement funds in South Africa have evolved over the last four decades - from defined benefit funds, to defined contribution funds with daily unit pricing, flexible benefit and investment options, and multiple opportunities to withdraw prior to retirement. With this evolution has come the need for more sophisticated IT systems to administer all the moving parts, and make sure they remain compliant.

The result is that today's retirement funds are part of a dynamic digital environment. To manage the risks and protect members' savings, we need a sound legal framework and a robust digital infrastructure.

Together, the Financial Sector Conduct Authority (FSCA) and the Prudential Authority (PA) have rolled out two game-changing Conduct Standards:

Joint Standard 1 of 2023: IT Governance and Risk Management (JS 1 of 2023), and

Joint Standard 2 of 2024: Cybersecurity and Cyber Resilience Requirements (JS 2 of 2024).

These standards aim to ensure that **financial institutions**, including retirement funds, implement effective IT governance, risk management, and cybersecurity measures to protect assets, secure sensitive data, and maintain operational continuity should something happen.

DEFINITION

What is a financial institution?

The definition of financial institution in the Financial Sector Regulation Act includes:

- Financial sector regulator: Includes bodies like the Financial Sector Conduct Authority (FSCA) and the Prudential Authority (PA).
- Financial product provider: Entities offering financial products, such as pension funds, insurance companies, or collective investment schemes.
- Financial service provider: Entities providing financial services, such as banks, financial advisors, or investment managers.
- Market infrastructure: Systems or entities facilitating financial transactions, such as stock exchanges or clearing houses.
- Holding company of a financial conglomerate: A parent company overseeing a group of financial entities.
- Person licensed or required to be licensed: Any entity or individual authorised or mandated to operate under financial sector laws, including retirement funds registered under the Pension Funds Act.

You can see from the definition of financial institutions, that these two Joint Conduct Standards apply not only to your retirement fund, but also to the majority of role players in your retirement fund's service provider eco-system.

Fund fiduciaries and decision makers, carry a lot of responsibility for ensuring compliance with these standards. This means making sure that the retirement fund's IT systems are sound and members' data is protected.

Don't worry if tech isn't your thing. This Trustee Tutor unpacks both Conduct Standards in a simple way, explains what they mean for you, and gives you practical tips to stay on top of things.

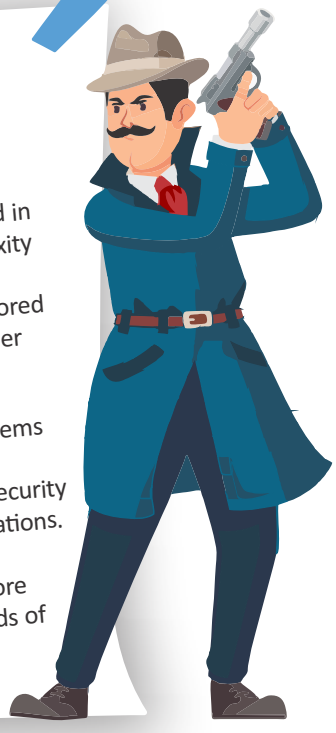
Before we get into the practical requirements, it's important to understand the level to which these Joint Standards apply to your fund. All retirement funds are different. They have different sizes of membership, different investments, and different levels of complexity. JS 1 of 2023 and JS 2 of 2024 are principle-based frameworks, which simply means that they allow flexibility for financial institutions to implement requirements that take into account their size, resources, and operational context. This approach of **proportionality** balances the need for robust oversight with the practical realities of diverse financial institutions.

DEFINITION

What is proportionality?

Proportionality refers to the principle that regulatory requirements and compliance obligations should be applied in a way that is appropriate for the nature, scale, and complexity of a financial institution's operations, risk profile, and importance. This ensures that the regulatory burden is tailored to the specific characteristics of a financial institution, rather than a one-size-fits-all approach.

For example, a large retirement fund with complex IT systems and significant assets under management would need to implement more sophisticated IT governance and cybersecurity measures compared to a smaller fund with simpler operations. Proportionality ensures that smaller funds are not overburdened with requirements designed for larger, more complex funds, while still maintaining adequate standards of risk management and security.



Having clarified this, let's get stuck in.

DEFINITION

The governing body of a retirement fund is the board of trustees.

Joint Standard 1 of 2023: IT Governance and Risk Management (aka getting your IT house in order)

Joint Standard 1 of 2023 was published in November 2023 and became effective on 15 November 2024. Think of it as the rulebook for how retirement funds (and other financial institutions like banks and insurers) should manage their IT systems by establishing a comprehensive framework for financial institutions to manage IT-related risks. Its aim is to mitigate risks that could lead to operational disruptions, reputational harm, regulatory non-compliance, or financial losses. In other words, prevent tech disasters that could mess up operations, damage your reputation, or even cost your fund big bucks.

The primary objective is to make sure that the **governing body** has, included in their governance and risk policies, a framework and procedure for handling IT risks, with clear rules and oversight to keep everything on track. It's not just about tech - it's also about making sure your retirement fund runs smoothly no matter what, enhancing operational resilience and member confidence.

What do you need to do?

JS 1 of 2023 outlines the following requirements for all financial institutions:

1 Set up an IT governance plan

- Retirement funds must set up a formal IT governance framework that defines roles, responsibilities, and oversight mechanisms. This framework must integrate IT risk management into the fund's broader risk management strategy.
- The board of trustees is accountable for approving IT strategies, policies, and ensuring effective oversight.

2 Establish an IT risk management framework

Develop a robust IT risk management framework to identify, assess, and mitigate risks. Key actions in this step are:

- Listing your IT assets (think computers, software, and data): know what you've got and how critical it is to the fund's ongoing business processes.
- Checking for risks: regularly considering what could go wrong, especially with third-party providers like administrators, is a requirement.
- Putting up guardrails: set up internal controls to keep your IT systems secure, reliable and resilient.

3 Plan for the worst – resilience and business continuity

- Put together an IT resilience plan to keep things running if something goes wrong, like a system crash or a power outage. Test this plan at least once a year with "what-if" scenarios.
- Ensure all data centres have backup power, cooling, and protection against hackers or natural disasters.

4 Oversight and accountability – who's responsible for what?

- Even if your fund outsources IT to a third party service provider, it's important to remember that you're still accountable for IT governance as the board of trustees. You need to make sure there's an appropriately skilled person or team handling the fund's IT risks.
- Regular reporting and updates to the board are a key requirement to keep everyone informed, in order to exercise proper oversight.

5 Policy documentation

- Document your fund's IT policies and processes, get them approved by the board, and review them regularly. These should reflect your fund's size, complexity, service delivery requirements and how much risk the board is willing to take.

What does this mean for trustees?

For retirement fund trustees, JS 1 of 2023 underscores your fiduciary duty to oversee IT governance and risk management.

Here's what you need to know:

- **You don't need to be a tech genius:** You don't have to code or fix servers, but you do need to make sure you have sufficient knowledge to ask the right questions in order to exercise appropriate oversight and risk mitigation. Undergo training and/or appoint expert advisors to help you.
- **Compliance is not negotiable:** Trustees are personally accountable for ensuring compliance. Non-compliance could potentially lead to penalties, reputational damage, or liability for any losses.
- **Outsourcing doesn't get you off the hook:** The vast majority of retirement funds appoint third party service providers for IT or administration services. However, trustees still need to monitor and make sure their appointed providers are following the rules, with clear service level agreements that detail all the service provider's responsibilities and obligations.
- **Sign off on policies:** Trustees are responsible for approving IT governance and risk management policies, ensuring alignment with the fund's operational needs and risk profile.

How to get started

Here's a quick checklist to help you assess your fund's compliance with 1 of 2023:

Joint Standard 2 of 2024: Cybersecurity and Cyber Resilience Requirements (aka locking down cybersecurity)

JS 2 of 2024 was released on 17 May 2024 and takes effect on 1 June 2025. This Conduct Standard is all about keeping your fund safe from cybercriminals who might try to steal data, scam members, or disrupt operations. It builds on JS 1 of 2023 by zooming in on cybersecurity and making sure your fund has the ability to bounce back from cyber-attacks with minimal impact to members' savings.

Trustees and management committees must keep in mind that retirement funds are attractive targets for hackers – these funds hold lots of personal information and manage huge sums of money. JS 2 of 2024 sets out clear steps to protect your fund and keep it running, even if something goes wrong.

What do you need to do?

JS 2 of 2024 breaks cybersecurity and resilience into seven key areas. Here's what you need to focus on:

1 Cybersecurity governance and strategy – set your cybersecurity game plan

- Create a cybersecurity strategy and review it every year to keep up with new threats. This strategy should cover how you'll protect your systems, allocate resources, and fix any weak spots.
- As trustees, you're in charge of making sure this plan is solid and that everyone knows their role, including third-party providers.

2 Asset identification and classification - know your assets

- Identify which business processes and information assets are most critical and need extra protection, for example member data and/or payment systems.
- Regular risk assessments of critical operations and assets are needed to safeguard against compromise.

3 Lock things down – protection measures

- Build security into your systems from the ground up (think “security by design”).
- Limit access to sensitive information with tools like multi-factor authentication (MFA), strong passwords, and controls for who can access what.
- Use encryption and data loss prevention to keep members' personal information safe.

4 Detection capabilities - spot trouble early

- Set up systems to detect weird or unusual activity, like someone trying to hack your network. This means using network security tools and detection software to identify and block malicious traffic.
- Run penetration tests and audits to validate the effectiveness of your controls.

5 Response and recovery - be ready

- The fund must have an incident response plan to make sure it acts quickly and effectively if there's a breach or incident. Serious cyber incidents need to be reported to the FSCA and PA within 24 hours.
- Keep secure backups of critical data so you can recover quickly if this information is lost or stolen.

6 Cybersecurity awareness and training - spread the word

- Have a cybersecurity awareness program to teach your team, trustees, and even members how to stay safe. For example, show members how to spot phishing emails or verify requests for their personal information.
- This is especially important for retirement funds, where members might not be tech-savvy and could fall for scams.

7 Information sharing and collaboration - team up

- Share info with other financial institutions and industry groups to stay ahead of new threats and learn what's working for others.

What does this mean for trustees?

JS 2 of 2024 significantly ramps up the pressure to keep your fund cyber-secure. Here's why it matters:

- **You could be liable:** If a cyberattack hits your fund and you haven't followed the standard, you might face fines or even personal responsibility for losses.
- **Your fiduciary duty to members:** Protecting members' personal and financial information is a key responsibility as a trustee. A breach could erode trust and hurt your fund's reputation.
- **Outsourcing is tricky:** While most retirement funds appoint third-party providers for IT and administration functions, trustees remain fully accountable for cybersecurity compliance.
- **More oversight needed:** You'll need to check that technical stuff like MFA and encryption is in place and that your incident response plan is in place.

How to get ready - Make sure you're compliant with JS 2 of 2024:

How JS 1 of 2023 and JS 2 of 2024 work together

Think of JS 1 of 2023 as the foundation of your house - it sets up the structure for managing IT risks and keeping things organised. JS 2 of 2024 is like the security system - locking the doors, installing alarms, and making sure you're ready if someone tries to break in. Together, they create a complete plan to keep your retirement fund safe and running smoothly.

Here's how they connect:

- **Start with governance (JS 1 of 2023):** This Conduct Standard gets your fund policies, sub-committees, and oversight responsibilities in place so you're ready to tackle IT risks.
- **Add cybersecurity (JS 2 of 2024):** This Conduct Standard brings in the technical tools and plans to fight off cyberattacks and recover to business as usual if something goes wrong.
- **You're always responsible:** Both Standards make it clear that the trustees are accountable for compliance, even if you outsource IT or administration services.
- **Tailor to your fund:** Both standards allow flexibility to tailor measures to your fund's size, complexity, and risk profile.

Let's look at this practically ...

Consider a retirement fund outsourcing IT and administration functions to a third-party service provider.

Under JS 1 of 2023, trustees must:

- Approve an IT governance policy outlining risk management processes.
- Ensure the provider's IT systems are secure and resilient, with regular risk assessments and testing.
- Consider establishing a sub-committee to oversee IT risk management.

Under JS 2 of 2024, trustees must:

- Verify that the provider implements MFA, encryption, and network security measures.
- Confirm the provider has an incident response plan and reports material cyber incidents to regulators.
- Provide cybersecurity awareness and training for staff and members to prevent phishing or fraud.

Non-compliance with either standard could expose the fund to cyberattacks, regulatory penalties, or reputational damage, with trustees facing potential liability.

Challenges you might face

Being a trustee isn't easy, and these standards come with some hurdles:

- **Tech can be daunting and confusing:** Not everyone is a tech whiz, and understanding IT risks or cybersecurity jargon can feel overwhelming.
- **Limited resources:** Smaller funds might struggle to pay for things like penetration testing or training programs.
- **Third parties add complexity:** Dependence on third-party service providers increases the complexity of ensuring compliance across multiple entities.
- **Hackers don't sleep:** Cyber threats are always evolving - think AI-powered scams or deepfake fraud - so you need to make sure you stay informed.
- **Regulators are watching:** The FSCA and PA are intensifying oversight, with annual compliance questionnaires and potential audits.

Tips to make this work

Here are some practical ways to tackle these standards and keep your fund compliant:

- **Get schooled:** Make annual refresher training part of your governance year plan to make sure you stay on top of the trends and latest scams. If you need help, bring in an expert who knows the ropes.
- **Leverage smart tools:** Look into affordable technology solutions for risk assessments, testing, or threat monitoring to save time and money.
- **Strengthen governance:** Consider incorporating IT and cybersecurity into an existing sub-committee's mandate or set up a separate committee to handle the details and report back to the board. Remember, this committee can be made up of experts who are not necessarily trustees.
- **Partner with providers:** Negotiate contracts that explicitly require compliance with both Conduct Standards, with regular reporting mechanisms.
- **Be part of the community:** Participate in industry forums to share threat intelligence and adopt best practices.
- **Keep good records:** Make sure you're ready for audits by the regulators by documenting everything - policies, risk assessments and incident response plans – demonstrating compliance.

Conclusion

Joint Standard 1 of 2023 and Joint Standard 2 of 2024 are your roadmap to keeping your retirement fund safe in a tech-driven world. The first sets up the rules for managing IT risks, while the second locks in cybersecurity and resilience to fend off hackers. Together, they make sure your fund is ready for anything, from system glitches to full-on cyberattacks.

As trustees, you've got a big job, but you don't have to do it alone. With some training, smart planning, and teamwork with your providers, you can meet these standards and protect your members' savings. Joint Standard 2 builds on the work you've done for Joint Standard 1, to make sure your fund is secure, resilient, and ready for the future.

Trustee Tutor 22:
IT governance and cybersecurity

How to?

The assessment for this issue of Trustee Tutor follows for information and/or training purposes. If you would like to earn verified CPD hours for reading this issue, please go to www.pensionsworldsa.co.za/cpd-portal/ and complete the assessment electronically to receive your certificate immediately on meeting the competency requirements.

1. Joint Standard 2 of 2024 on Cybersecurity and resilience has been issued jointly by:

a. The Financial Sector Conduct Authority & the Office of the Pension Funds Adjudicator ☐
b. The Financial Sector Conduct Authority & the Prudential Authority ☐
c. The Prudential Authority & the South African Revenue Services ☐
d. The South African Revenue Services & the South African Reserve Bank ☐

2. Joint Standard 1 of 2023 and Joint Standard 2 of 2024 apply to all financial institutions. In this context, financial institutions includes:

a. Retirement funds ☐
b. Banks ☐
c. Investment managers ☐
d. All of the above ☐

3. JS 1 of 2023 and JS 2 of 2024 are principle-based frameworks, which simply means that they allow flexibility for financial institutions to implement requirements that take into account their size, resources, and operational context.

a. True ☐
b. False ☐

4. Choose the incorrect answer. The primary objective of Joint Standard 1 of 2023 on IT Governance and risk management is to ensure that retirement funds have:

a. A framework and procedures for handling IT risks ☐
b. Set up internal controls to keep the fund's IT systems secure, reliable and resilient ☐
c. Put together an IT resilience plan to keep things running if something goes wrong ☐
d. Delegated the accountability for IT governance and risk management to any third party service providers or sub-contractors used ☐

5. IT assets are:

a. Furniture, vehicles and people ☐
b. Telephones, fax machines and intellectual property ☐
c. Computers, software and data ☐
d. Those people who keep the organisation's passwords safe ☐

6. Compliance with Joint Standard 2 of 2024 on Cybersecurity and resilience is effective for all relevant financial institutions on:

a. 1 May 2025 ☐
b. 1 June 2025 ☐
c. 1 July 2025 ☐
d. 12 months from 1 June 2025 ☐

Trustee Tutor 22:
IT governance and cybersecurity

7. In terms of Joint Standard 2 of 2024, retirement funds need to:

a. Set up a cybersecurity strategy ☐
b. Review their cybersecurity strategy annually ☐
c. Set up an IT/Cyber Sub-Committee ☐
d. a and b only ☐

8. Serious cyber incidents need to be reported to the FSCA and PA within __ hours

a. 24 ☐
b. 48 ☐
c. 72 ☐
d. Depends on the severity of the incident ☐

9. According to Joint Standard 2 of 2024, retirement funds need to set up tech defenses. These include:

a. Multi-factor authentication ☐
b. Encryption ☐
c. Network security ☐
d. All of the above ☐

10. In terms of Joint Standard 2 of 2024 financial institutions are expected to participate in industry forums to share threat intelligence and adopt best practices.

a. True ☐
b. False ☐