seshego consulting

insights

never be in need

MAY 2023: EDITION 4 of 2023

In case you missed it…

1. April 2023: Sustainability of Retirement Funds – an Overview
2. March 2023: Deductions in terms of Section 37D of the PF Act
3. February 2023: Budget summary 2023/2024 Tax Year

DRAFT CONDUCT STANDARDS ISSUED BY THE FINANCIAL SECTOR CONDUCT AUTHORITY AND THE PRUDENTIAL AUTHORITY

1. Draft Prudential Standard ("the Prudential Standard") on Reporting in terms of Regulation 28 of the Pension Funds Act.

1.1 The purpose of Regulation 28, which forms part of the Regulations to the Pension Funds Act, 1956 ("the PF Act") is to provide prudent investment guidelines to the trustees of a retirement fund. Regulation 28 aims to protect members' benefits from the effect of poorly diversified investment portfolios.

Thus Regulation 28 limits the exposure of the fund's assets to a particular asset or asset classes. Regulation 28 also requires the trustees to consider factors that may influence the sustainable long-term performance of the fund's investments, such as factors of an environmental, social, and governance nature.

1.2 Prior to the Prudential Standard on Regulation 28, retirement funds were required to report instances of non-compliance to the Financial Sector Conduct Authority ("FSCA"). The most significant change made by the Prudential Standard is that the FSCA now requires reporting on compliance with Regulation 28.

1.3 Therefore, going forward, a retirement fund will have to submit a full report each quarter on its compliance with Regulation 28 to the FSCA. This will mean a great deal of extra work for retirement funds, especially as the exclusion from the look-through approach no longer applies to Collective Investment Schemes and insurance policies.

It will also increase costs. It is unlikely that this additional work will be covered by the current administration fee, so the retirement fund will incur an additional expense in order to comply with this requirement.

1.4 The Prudential Standard requires the reporting to be done quarterly and therefore each quarter is defined in the standard. For example, the first quarter means from 1 January to 31 March of each year, and so on. However, for 2023, the report for the first quarter ending 31 March 2023 must be submitted on or before 30 September 2023 and for all subsequent quarters, the report must be submitted within 90 days after quarter end.

1.5 Certain terminating funds are exempt from the reporting requirements. Terminating funds that have appointed a liquidator, or have been exempted from liquidation or where a full transfer of assets and liabilities has been approved by the FSCA do not need to comply with the reporting requirements.

1.6 The Institute for Retirement Funds Africa ("IRFA") is asking the FSCA to consider combining reporting on compliance with Regulation 28 with the quarterly report to the South African Reserve Bank.

Rationalising the two processes would reduce the work involved but we do not know at this stage whether the IRFA has had any success. Given that the draft Prudential Standard requires the report for the first quarter of 2023 to be submitted by 30 September 2023, it is to be hoped that the Prudential Standard and any associated guidelines will be finalised in the near future.

We will advise you as soon as further information is forthcoming.

2. Draft Joint Standard on Cyber Security and Cyber Resilience Requirements ("the Joint Standard")

2.1 Objective of the Joint Standard

The stated objective of the Joint Standard is to set out the minimum requirements for sound practices and processes of cybersecurity and cyber resilience. It is the responsibility of the governing body of a financial institution to ensure that the financial institution meets the requirements set out in this Joint Standard on a continual basis.

The Joint Standard addresses requirements relating to governance, cybersecurity strategy and framework, cybersecurity and cyber resilience fundamentals, cybersecurity hygiene practices, as well as regulatory reporting.

The definition of a financial institution in the Joint Standard now includes a pension fund registered in terms of the Pension Funds Act. Although the term "senior management" is defined in the Joint Standard, the term governing body is not. However, it is clear that in relation to a retirement fund, the governing body is the board of trustees. Compliance with the standard carries a level of risk for the trustees, especially as there are areas where the trustees are required to use their discretion. Therefore there is a risk for the retirement fund if they use that discretion incautiously.

Since this is a Joint Standard, it applies to banking institutions as well as the areas in the financial sector regulated by the FSCA. The term "Authorities" in the Joint Standard is defined to include the Prudential Authority as well as the FSCA.

2.2 What are the minimum requirements?

The minimum requirements are in fact very extensive. The financial institution must inter alia:

- establish and maintain a cyber security framework and must review its strategy annually;
- protect the cyber security of the fund by implementing appropriate and effective cyber resilience capabilities and practices to limit or contain the impact of a potential cyber event;
- take the measures listed in the Joint Standard to protect its data security, its access and system security, and its network security;
- establish an incident response and management plan;
- regularly test the effectiveness of all elements of its cyber resilience capacity and security controls;
- maintain cybersecurity hygiene practices, which would include managing access to its systems by establishing a password policy and a process to enforce strong password security controls for users;
- notify the Authorities in the form and manner determined by the Authorities, of any material systems failure, malfunction, or other disruptive event within 24 hours of classifying the event as material.

2.3 Risks for the Trustees in Implementing the Joint Standard.

2.3.1 Cyber-attack is on the rise globally, with cyber criminals devising ever more sophisticated methods of hacking into the systems of financial institutions. The need for retirement funds to comply with the requirements of the Joint Standard is self-evident but there are a few areas which may require clarification.

2.3.2 Clause 3.5 of the Joint Standard states that:

> *"The requirements of this Joint Standard must be implemented in accordance with the risk appetite, nature, size and complexity of a financial institution."*

This clause implies that the trustees as the governing body must apply the concept of proportionality in relation to the implementation of the minimum requirements. Does this mean that a smaller retirement fund is required to have less stringent controls in place than for example a large commercial umbrella fund?

2.3.3 Clause 10 requires that a material incident must be reported to the Authorities within 24 hours of the occurrence of the incident. However, the term "material" is not defined in the standard and the decision with regard to what constitutes a material breach of cyber security rests with the board of trustees.

2.3.4 The Joint Standard makes it clear that the responsibility for oversight of compliance with the minimum requirements lies with the governing body. In practice, however, the board of trustees delegates all functions related to the day-to-day running of the fund to an administrator.

In turn, administrators may outsource certain functions, in particular the IT function to a third party.

As the governing body, the trustees need to review their service level agreement with the administrator to ensure that the administrator has agreed to maintain cyber security processes and hygiene practices that are aligned with the minimum requirements prescribed by the Joint Standard.
The trustees may also need to scrutinise the administrator's agreement with third-party service providers such as the IT company used by the administrator.

2.3.5 The Joint Standard requires that cybersecurity must be maintained on a continual basis.

Therefore, once the Joint Standard is finalised and legislated, it is recommended that the trustees should review the agreements mentioned in paragraph 2.3.4 above annually.

Should you have any questions regarding the above, please contact your consultant to assist you.