DASHBOARD
LEGAL UPDATES

EDITION 05 | MARCH | 2022

1. The offshore limit for retirement funds
2. FCSA Information Request 2 of 2022 withdrawn for now
3. Draft Joint Standard on cybersecurity and cyber resilience requirements
4. Office of the Pension Funds Adjudicator Communication 1 of 2022 - revised turnaround times for responses

1. The offshore limit for retirement funds

2022 Budget Review

On 23 February 2022, the Minister of Finance, Enoch Godongwana, included the following in the 2022 Budget Review:
"Institutional investors
The offshore limit for all insurance, retirement and savings funds is harmonised at 45 per cent inclusive of the 10 per cent African allowance. The previous maximum limits were set at 30 per cent or 40 per cent for different investors."
Included within the meaning of "institutional investors" is retirement funds.

South African Reserve Bank (SARB) Circular

Shortly after the Budget Review, the SARB issued Exchange Control Circular 10/2022, dated 23 February 2022.
The SARB Circular provides that:

"…that with effect from 2022-02-23, the prudential limits of 30 per cent and 40 per cent, respectively as well as the African allowance of 10 per cent have been **combined into a single limit of 45 per cent** of total retail assets under management, applicable to all qualifying institutional investors". (Own emphasis.)

This is reflected in the following amended wording of the limit:
"Prudential limit: the foreign exposure of retail assets may not exceed: 45 per cent in the case of pension funds; the linked and non-linked business of life insurers; CIS managers; and discretionary financial services providers registered as institutional investors with the Financial Surveillance Department".

Rest of Africa limit fallen away but reporting remains

It is clear that the rest of Africa limit of 10 per cent has fallen away and a single overall offshore limit now applies. SARB states that:

"The prudential limits of 30% and 40%, respectively as well as the African allowance of 10% have been **combined into a single limit of 45%".** (Own emphasis.)

However, please note that SARB states in the Circular that for statistical purposes the *reporting of the African exposure* on the quarterly asset allocation report will remain.

For the submission of the quarter end December 2021 quarterly asset allocation reports, the limits of 30 per cent and 40 per cent respectively as well as the 10 per cent African allowance, will still be applicable.

Regulation 28 provides for SARB to set the limit, thus an amendment of regulation 28 is unnecessary

Regulation 28 provides that: the aggregate exposure to foreign assets, referred to in [the Regulation 28 table] and expressed as a percentage, must not exceed the maximum allowable amount that a fund may invest in foreign assets *as determined by the South African Reserve Bank*, or such other amount as may be prescribed.
Thus, SARB has the authority to determine the limit without an amendment to Regulation 28.

Financial Sector Conduct Authority (FSCA) Communication 8 of 22 (Retirement Funds)

On 18 March 2022, the FSCA issued a communication confirming the offshore limit as determined by SARB. The communication does not contain additional information.

The communication provides that: "Where necessary, the Board of the fund may revise their investment policies and mandates in accordance with the principles contained in Regulation 28".

2. FSCA Information Request 2 of 2022 withdrawn for now

The FSCA issued Information Request 2 of 2022 on 7 March 2022. The Information Request required the mandatory online submission, by retirement funds and administrators, of information about unclaimed benefits and paid-up members.
The FSCA has withdrawn this Information Request for now since old versions of the annexures were published with the Information Request.

3. Draft Joint Standard on cybersecurity and cyber resilience requirements

The FSCA and the Prudential Authority (**PA**) (**Authorities**) have published, for consultation, the draft Joint Standard entitled Cybersecurity and Cyber Resilience Requirements. The Joint Standard is issued by the Authorities in terms of their powers under the Financial Sector Regulation Act. A Joint Standard (once published and effective) is compulsory (law) and must be complied with by the persons to whom it applies. Persons to persons to whom it applies.

The authorities state that they are unable, at this stage, to ascertain the full extent of the expected impact of the draft Joint Standard on financial institutions. As part of the consultation process, the Authorities have solicited industry inputs on the expected impact of implementing the proposed Joint Standard.

Some useful definitions:

- **Cyber**: the medium of the interconnected information infrastructure of interactions among persons, processes, data, and IT systems.
- **Cybersecurity**: the preservation of confidentiality, integrity and availability of information or IT systems through the cyber medium. In addition, other properties such as authenticity, accountability, non-repudiation, and reliability can be involved.
- **Cyber resilience**: The ability of a financial institution to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents

The Joint Standard, and the joint communication about the draft Joint Standard issued by the Authorities, is available on their websites.

It is likely that there will be a second draft issued for another round of consultation.

What is the overall aim of the Joint Standard?

The aim of the Joint Standard is to ensure that financial institutions have adequate cybersecurity and cyber resilience practices

The communication about the Joint Standard provides that: "The draft Joint Standard seeks to ensure that these financial institutions implement processes and have tools and technology which will prepare them for cyber-attacks as well as respond to and recover from such attacks".

To which financial institutions will the Joint Standard apply?

The Joint Standard will apply to the following financial institutions:

Retirement funds	Discretionary Financial Services Provider (**FSP**)
Managers of collective investment schemes	Administrative FSP
Banks (and branches), branches of foreign institutions and controlling companies	Insurers and controlling companies
Mutual banks	Over-the-counter derivative providers
Market infrastructure	

Who is responsible to ensure compliance with the Joint Standard?

The governing body is ultimately responsible for ensuring that the financial institution complies with the requirements set out in the Joint Standard and the oversight of cyber risk management (but may delegate primary oversight activities to a committee). The governing body of a retirement fund is its board.

The governing body together with senior management must, among other things, ensure that a sound and robust cybersecurity strategy and framework is established, implemented, and maintained.

Proportionality

The Joint Standard allow for a proportional application of the requirements as they must be implemented commensurate with the risk appetite, nature, size, and complexity of a financial institution.

Requirements

The requirements set out in the Joint Standard are wide-ranging and include the following topics:

Roles and responsibilities	Cybersecurity and cyber resilience fundamentals
Governance	Access management
Cybersecurity strategy and framework	Privileged access management
Identification	Multi-factor authentication
Protection	Network perimeter defence
Detection	Vulnerability and patch management
Response and recovery Situational awareness	Secure configurations Malware protection
Testing	Cybersecurity hygiene practices
Learning and evolving	Regulatory reporting

We cannot cover all the requirements in this *Dashboard* and will provide a more comprehensive summary once the Joint Standard is finalised. Some examples of the requirements are set out below.

Governance requirements

A financial institution must (among other things)-

- clearly define the roles and responsibilities of all management and oversight functions as well as committees established for the purposes of exercising oversight of cyber risks;
- ensure cyber risk management is incorporated into the governance and risk management structures, processes, and procedures of a financial institution;
- ensure that an information security function with adequate resources, appropriate authority, and access to the governing body is established where applicable; and
- ensure that the governance and oversight of the information security function is independent from operations.

Cybersecurity strategy and framework

A financial institution must (among other things)-

- establish and maintain a cybersecurity strategy that is approved by the governing body;
- establish a cybersecurity framework to manage cyber risks;
- align its cybersecurity framework with its enterprise risk management framework;
- establish cybersecurity policies, standards and procedures that are informed by industry standards and best practices to manage cyber risks and safeguard information assets;
- annually define and quantify business risk tolerance relative to cybersecurity and ensure that it's consistent with the business strategy and risk appetite; and
- establish metrics to gather information that enables reporting at both a technical and executive-level across all aspects of its cyber risk management implementation programme.

Regulatory reporting and notification

The Joint Standard includes requirements for financial institutions to notify the Authorities of material system failure, malfunction, delay, disruptive event, or cyber incident within 24 hours of the event being classified as 'material'.
The Authorities may determine the regulatory reporting required by financial institutions in relation to requirements of the Joint Standard.

4. Office of the Pension Funds Adjudicator (OPFA) Communication 1 of 2022 – revised turnaround times for responses

On 28 March 2022, the Pension Funds Adjudicator (**Adjudicator**) issued this communication. In Communication 2 of 2021, the OPFA instituted a process whereby if members had not first approached the relevant fund before approaching the OPFA to complain, the OPFA would facilitate this approach. The OPFA does this by giving the parties 30 days to try to resolve the complaint, which is called the 'refer to fund approach' (**RTF**).

The Adjudicator remarks that the RTF is working well. However, that because funds are aware of the complaint, as a result of the RTF, if the RTF does not result in the complaint being resolved to the satisfaction of the complainant, a further 30 days to respond formally is not necessary. In the past the turnaround time for the formal response from the fund/employer was 30 days. A further 14 days was provided if the response was not received.

From **1 April 2022** , the turnaround times for a formal response will be **20 days** with a further **10 days** if a response is not received.