South Africa: Insurance industry update

August 2024

Milliman

David Kirk, FASSA
Susan Melmed, FASSA
Adél Drew, FIA
Gaël Neuhaus
Cameron Hollaway

IN THIS UPDATE:

- Recent wave of regulatory releases
- Embedding climate-related risks in a risk management framework
- Lessons learnt from CrowdStrike
- South Africa's new streamlined complaints framework
- Guarding gold: The role of insurance in the Olympic Games

Introduction

In this issue, we delve into the recent wave of releases from the Prudential Authority (PA) and the Financial Sector Conduct Authority (FSCA), with a focus on emerging risks including outsourcing risk, cyber risk, and climate risk. We look into the new structure of delivering formal complaints to the ombuds as well as what role insurance plays in the Olympic Games.

If you want to receive our Industry Update and other relevant publications regularly, please send a request to africa@milliman.com.

Recent wave of regulatory releases

May was a busy month for the PA and FSCA with the release of regulations and guidance applicable to insurers on liquidity risk, outsourcing risk, cyber risk, and climate risk.

DRAFT LIQUIDITY RISK PRUDENTIAL STANDARD AND GUIDANCE NOTE

The proposed Liquidity Risk Prudential Standard (FSI 6) issued by the PA is a complete overhaul of the current FSI 6 to bring it in line with emerging international practice.

- It now includes detailed requirements on the governance and risk management of liquidity risk, including a Board-approved contingency funding plan that is to be tested annually.
- The LIQ metric will be replaced with the more detailed Insurance Liquidity Ratio (ILR) that is assessed over different time horizons.
- Additional liquidity risk reporting to the PA (beyond the ORSA) will be required in the form of a monthly liquidity return and an annual Board-approved Liquidity Risk Management Report.

Comments were due to the PA by 31 July 2024.

JOINT STANDARD ON OUTSOURCING BY INSURERS

This new standard issued by the PA and FSCA replaces the Prudential Standard GOI 5 (Outsourcing by Insurers) issued by the PA. It now allows for a regulatory framework governing outsourcing by insurers from both a prudential and conduct perspective.

Some of the additions compared to GOI 5 include requirements relating to terminations, including credit risk and conduct risk in risk assessments, as well as regular review of outsourced providers' contingency plans.

This new standard comes into effect 1 December 2024. Insurers should note that prior outsourcing arrangements must comply with this new standard within 24 months of the effective date or upon renewal/renegotiation, whichever comes first.

JOINT STANDARD ON CYBERSECURITY AND CYBER RESILIENCE

This is a new standard issued by the PA and FSCA setting out minimum requirements for sound practices and processes relating to cybersecurity and cyber resilience for all financial institutions (including banks, insurers, and their controlling companies).

The commencement date is 1 June 2025.

It is likely that larger players already meet most of these requirements, which are in line with industry good practice. However, other insurers may have more gaps to close despite the standard's allowance for the implementation to reflect the nature, size, complexity, and risk profile of the entity.

We recommend performing a gap analysis as soon as possible to establish the extent of any gaps and allow sufficient time to close these. Also keep in mind the IT Governance and Risk Management Joint Standard that was released last year with an effective date of 15 November 2024.

CLIMATE RELATED GUIDANCE NOTES

The PA has issued Guidance on climate-related disclosures for Insurers and Guidance on climate-related governance and risk practices for insurers. We discuss these in the next section as well as here.

Embedding climate-related risks in a risk management framework

While current guidelines from the PA on managing climate-related risks are not mandatory, the PA has indicated that they will be monitoring implementation closely. These guidelines, therefore, could become mandatory if organisations do not make sufficient progress.

Many organisations start with embedding climate using a bottom-up approach, focusing on individual asset classes or liability level. However, a more holistic approach aligned to an organisation's objectives is essential for the entire risk management control cycle, i.e., assess, manage, monitor, and report.

A key starting point for embedding climate-related risks into a Risk Management Framework (RMF) is to consider the business strategy and define a clear climate strategy and governance structure. Establishing a unified language around climate risks is crucial for embedding these risks into the business, and lastly integrating into the organisation's controls, with effectiveness ensured through internal audits.

In overseas markets with established climate regulations, sustainability has become a broader theme that surpasses climate-only discussions, encompassing social consequences of transitioning from fossil fuels and the impact on nature. For those at the beginning stages of their climate journeys, adopting a broader sustainability focus may offer a competitive advantage in the long run.

STRATEGY

A well-defined climate strategy set by the Board is essential for managing climate-related risk, ensuring coherence and consistency across the organisation. This strategy should translate into specific risk appetite statements aligned with the overall business strategy.

GOVERNANCE

Effective governance ensures comprehensive understanding, oversight, and accountability for climate-related risks. Governance structures should be robust and clearly defined, starting at the Board level and cascading through the organisation.

RISK TAXONOMY

New terminology may be required to accurately describe how climate impacts traditional risk categories. Explicitly outlining these factors within traditional categories can help the organisation become climate literate. It is also worthwhile to consider whether new risk categories are needed and ensure taking steps to ensure a unified vocabulary for clarity and consistency.

CASCADING THROUGH THE RMF

With the direction set in terms of strategy and how to describe and categorise climate-related risks, it is then possible to cascade these through the rest of your risk management framework, tools, processes, and technologies. The easiest approach to doing this is to systematically review all existing policies, processes, and controls, explicitly adding climate considerations where relevant.

ASSURANCE

Regular audits and reviews ensure that risk management activities are effective and aligned with the climate strategy. Monitor how the business incorporates evolving climate risks and update key assumptions and approaches regularly.

Embedding climate-related risks into an RMF requires a strategic, well-governed, and holistic approach. Without this strategic direction, different functions within the organisation might develop varying approaches towards managing climate risk, leading to ambiguity and inconsistency in direction and priorities.

Milliman's Climate Benchmarking Survey, with results expected in Q3, will help insurers benchmark their progress. To receive a summary of these results please send a request to adel.drew@milliman.com.

Lessons learnt from CrowdStrike

On 19 July, the world was at a standstill as the cybersecurity company CrowdStrike implemented a software update that crashed over 8 million computers worldwide. The global outage resulted in business disruption, interrupting essential services and costing companies millions of dollars, affecting companies such as airlines, banks, hospitals, and emergency lines. CrowdStrike, previously held in high esteem, saw their share price fall by about 32% over the following 12 days and have now been sued by their shareholders for materially false and misleading assurances about its technology.

RESPONSE AND RECOVERY

In May, the PA and FSCA released a joint standard on cybersecurity and cyber resilience, outlining steps financial institutions must take to protect themselves and their clients. A key focus of the standard is on how to effectively respond to and recover from cyberattacks or systemic failures. It mandates that entities should have capabilities in place to rapidly respond and recover, along with regular backup strategies to ensure business continuity and minimise customer impact.

Despite CrowdStrike rolling back the update just an hour and a half after its release, the damage had already been done. The software had crashed all Microsoft Windows PCs globally that had their Falcon software installed, leading to widespread "blue screen of death" errors. Remedies to these errors were found much later in the day, when IT departments of affected companies had to develop their own solutions by repeatedly rebooting the PCs. This incident highlights the importance of thorough software testing and robust recovery measures, as CrowdStrike was unable to assist its customers effectively with their own product. It serves as a case study highlighting the necessity of having a well-defined procedure for responding to and resolving cyberattacks and system failures, as emphasised in the joint standard.

THE USE OF THIRD-PARTY SERVICES

The joint standard also addresses the use of third-party service providers for managing IT systems or information assets. It requires financial institutions to be satisfied with the nature and frequency of testing controls. Institutions should develop policies and procedures to ensure that any code updates are subject to review and testing, both internally and by the provider, before integration into their software systems.

It remains unclear whether the entities affected by the CrowdStrike incident had policies in place to prevent the rollout of untested software updates. However, the incident highlights the critical importance of internal testing of third-party systems before deploying them across an organisation. Such practices are essential for mitigating business interruptions and enhancing cybersecurity hygiene.

South Africa’s new streamlined complaints framework

The 2023 joint annual report from the Ombudsman for Long-term Insurance (OLTI) and the Ombudsman for Short-term Insurance (OSTI) will be the last of its kind. As of March 2024, these reports will be consolidated with two other Ombudsman reports to form part of the newly established National Financial Ombud Scheme South Africa (NFO).

WHY THE CHANGE?

The NFO will assume responsibility for four previously separate industry ombud schemes: the Ombudsman for Banking Services South Africa, the Credit Ombud, OLTI, and OSTI. This significant change stems from the recommendations of a World Bank report published in 2021. The report scrutinised the role of the financial sector ombud system in South Africa and recommended that reform was necessary to align the system with the complexities of the South African financial sector and ensure that it is fit for purpose.

In response to these recommendations, the NFO represents a voluntary amalgamation of the four aforementioned ombuds. This unified scheme aims to streamline operations, enhance efficiency, and better serve the needs of South African financial consumers by creating a more cohesive and effective ombud system.

The formation of the NFO signifies a shift in the financial sector's approach to dispute resolution and consumer protection. By integrating these separate entities, the NFO is poised to offer a more streamlined and coordinated dispute resolution framework, ultimately benefiting consumers and the industry alike.

OLTI AND OSTI ANNUAL REPORT

With the recent release of the OLTI and OSTI 2023 annual reports, insurers would have been hoping to avoid being included in the ensuing news articles of the most complained-about insurers in 2023. While some insurers couldn’t avoid this, others were able to leverage these reports to show off their low Ombudsman complaints.

The OLTI report indicated that complaints made regarding declined claims were dominated, again, by those in relation to funeral benefits. Overall, the total number of complaints declined in 2023; however, OLTI complainants received more in payouts compared to 2022 (R283 million versus R201 million).

Conversely, the OSTI report shows that a higher number of new claims were registered in 2023 compared to 2022, with motor vehicle insurance making up the greatest proportion of these. Most of these vehicle complaints related to declined accident-related claims due to an exclusion in the policy. Exclusions included a lack of due care or precaution in preventing or minimizing the loss, misrepresentation or non-disclosure at the time of taking out the policy, and at claim’s stage.

The formation of the NFO aims to maintain strong emphasis on promoting good market conduct among financial institutions, thereby bolstering consumer confidence in the financial sector. The NFO will provide a more streamlined and less confusing dispute resolution framework for financial consumers, though ideally, only a limited number will need to utilise these services.

Guarding gold: The role of insurance in the Olympic Games

While watching the pole vaulting and gymnastics at the Olympic Games, one might wonder what kind of risks are involved and what type of insurance does this global event have? In the 2016 Rio de Janeiro Summer Olympics, we saw 8% of athletes injured and 5% incurring illness, while in the 2020 Tokyo Games approximately 9% were injured with a further 4% falling ill. How do the Olympians and the organisers guard themselves against potential mishaps?

ALLIANZ OLYMPIC GAMES PARTNERSHIP

Building on their collaboration with the Paralympic Movement since 2006, Allianz entered an eight-year worldwide partnership with the Olympic and Paralympic Movements in 2021. The partnership includes liability, cyber, and property damage cover to the International Olympic Committee (IOC) for several venues during the games in any location. The partnership also includes cover for any medical assistance required by staff, athletes, and volunteers during the games, as well as personal accident insurance for the national teams. Allianz even goes as far as to insure fans for ticket cancellations if they are unable to attend the games. The list of insured events includes everything from illness or injury to unexpected work commitments.

COVERING AN OLYMPIAN

While Allianz provides substantial coverage during the games, athletes need to ensure that they are protected beyond the event.

Income protection and disability insurance: Olympians push their bodies to the limit, increasing their risk of career-threatening injuries. The payout is generally tailored to help the athlete manage the financial transition from being a high-performing athlete to the next phase of their life.

Health insurance: Given that an Olympian pushes their body to the extreme, the need for health cover is not your average insurance policy. The cover will usually include hospital visits and procedures as well as specialised rehabilitative services and should allow for coverage globally.

Liability insurance: This is particularly important for all sports, particularly those as physical and competitive as martial arts. If you injure another athlete, you may be legally liable to compensate for inadvertent injuries.

Travel insurance: With all the travelling from competition to competition, there will likely be a flight missed or suitcase missing. Unfortunately, for the Olympian it is not as casual as the average holiday-goer, given the frequency of travel and the costs of their gear, as well as the repercussions if an event is missed.

Equipment insurance: Many athletes have specialised equipment, often custom-made and niche. The Japanese Olympic track bike V-IZU TCM2 frameset, for example, is priced at a staggering €126,555. Beyond normal wear and tear, as well as theft considerations, it is vital to have an athlete’s equipment insured.

How Milliman can help

- Dealing with regulatory change and approvals
- Iterative Risk Margin implementation, review, and applications to the PA
- Modelling of life insurance claim variability to inform reinsurance requirements
- Climate risk management support, including the development of decision-useful climate scenarios
- Independent views and reviews, of Heads of Actuarial Function, ORSAs, policies, first line actuarial processes, and for Section 50 transfers
- Analysing non-life claims volatility and assessing potential for ISPs to lower capital, or alignment of IFRS17 risk adjustment, SAM standard formula, and actual claims volatility
- Implementation of tried and tested methods for managing complex and emerging risks
- Conversion of Excel spreadsheets into powerful, cloud-based models with all the features of alternative proprietary software using Milliman Mind
- Review of product management (performance, distribution and retention, risk, TCF, and premium reviews)

Milliman

Milliman is an independent consulting, benefits and technology firm. Our expert guidance and advanced analytical solutions empower leading insurers, healthcare companies and employers to protect the health and financial well-being of people everywhere. Every day, in countries across the globe, we collaborate with clients to improve healthcare systems, manage risk, and advance financial security, so millions of people can live for today and plan for tomorrow with greater confidence.

milliman.com

CONTACT

David Kirk
david.kirk@milliman.com

Susan Melmed
susan.melmed@milliman.com

Adél Drew
adel.drew@milliman.com

Gaël Neuhaus
gael.neuhaus@milliman.com

Cameron Hollaway
cameron.hollaway@milliman.com