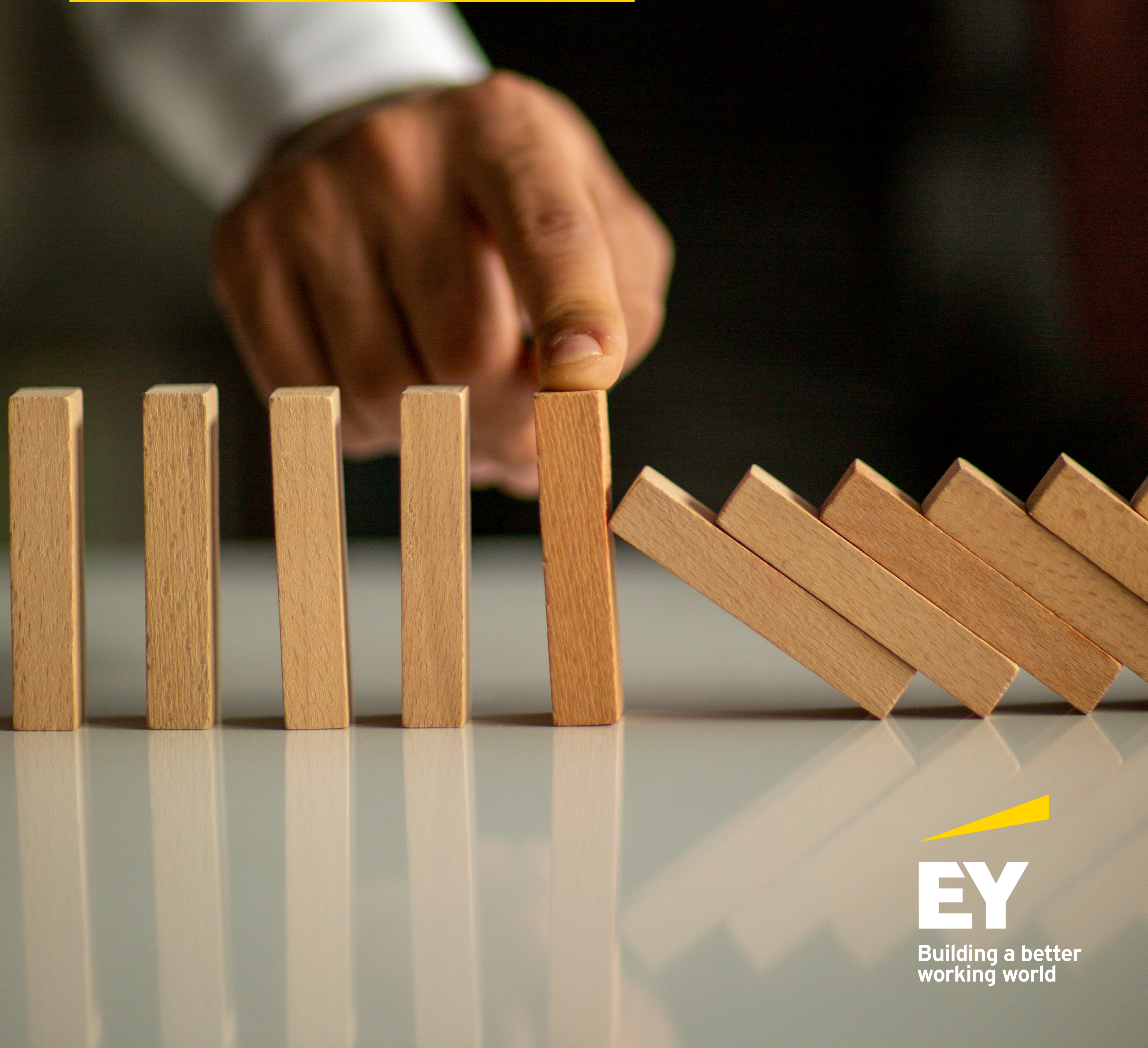
Regulatory Developments in Insurance

Newsletter

July 2021



Building a better working world

Contents

Please click on below topics to read more

Current Regulatory Developments

Prudential Regulations

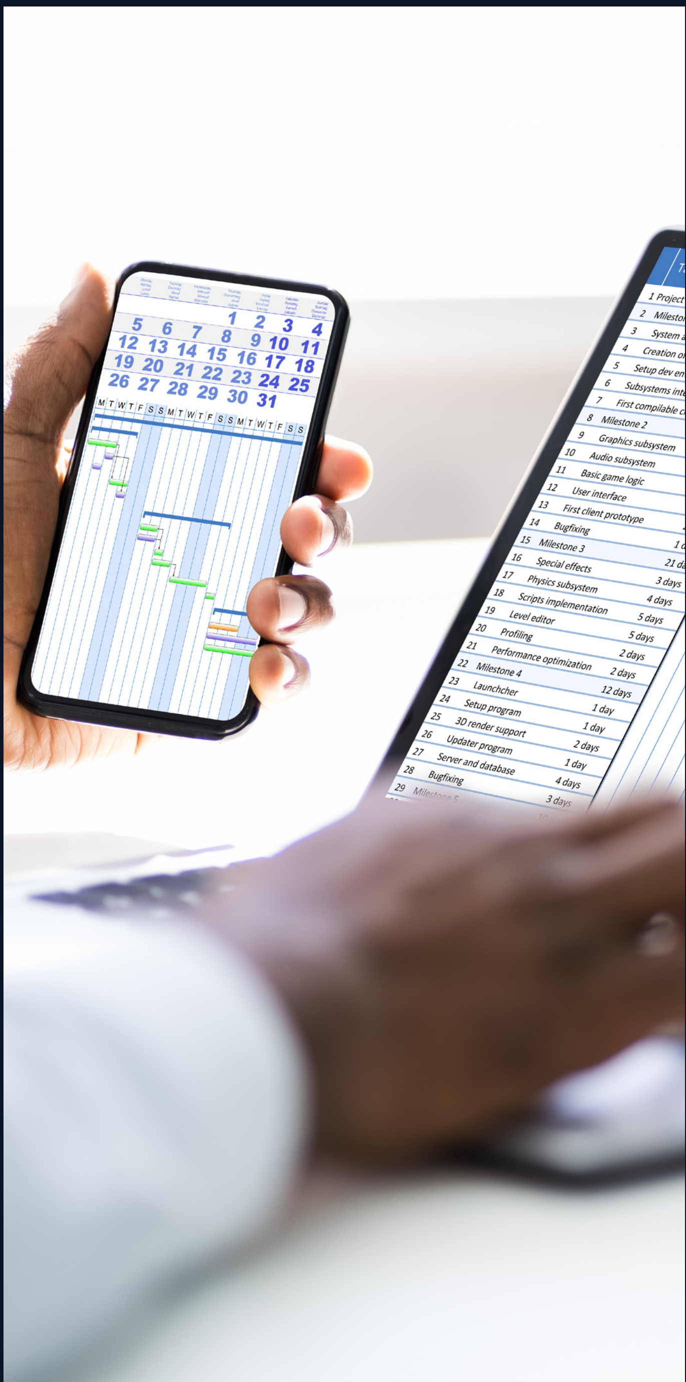
Regulatory reform	Implementation date
Guidance Note 1 of 2021 - Guidance on Iterative Approach for determining the Solvency Capital Requirement using the technical provisions including the risk margin (Insurance Act, 2017 – Addition to Guidance Notice to FSI 2.2, Chapter 10)	March 2021
Prudential Standard – Audit Requirements for Insurers;	2021
Prudential Standard – Audit requirements for Groups;	2021
Prudential Standard – Audit requirements for Lloyds;	2021
Prudential Standard – Audit requirements for Microinsurers;	2021
Prudential Standard – Audit requirements for Branches;	2021
Draft Guidance Notice 1 of 2020 - Audit requirements for entities registered under the Insurance Act, 2017	2021
Designation as a Systemically Important Financial Institution (D-SIFI)	Expected 2021

Conduct Regulations

Regulatory reform	Proposed implementation date
Conduct Standards – Requirements related to third party cell captive insurance business	2021
COFI	2022

01

Cell Captive Insurance Conduct Standards



A cell captive insurance structure is a type of insurance where the owner of the cell:

(a) holds an equity participation in a specific class or type of shares of an insurer, which equity participation is administered and accounted for separately from other classes or types of shares;

(b) is entitled to a share of the profits and liable for a share of the losses as a result of the equity participation referred to in paragraph (a), linked to profits or losses generated by the insurance business referred to in paragraph (c); and

(c) places or insures insurance business with the insurer referred to in paragraph (a), which business is contractually ring-fenced from the other insurance business of that insurer for as long as the insurer is not in winding-up.

The Insurance Act, 2018, introduced licensing and prudential requirements for cell captive insurers, however, the Regulator noted there was a gap in terms of conduct related legislation. This culminated in the draft cell captive conduct standards which were published for comments during 2020. In its statement in support of the conduct standards, the FSCA noted various risks associated with cell captive insurance structures. One key risk that stands out is the risk of insurers not taking sufficient responsibility for, and exercising adequate oversight of, the conduct of cell owners in relation to the fair treatment of policyholders. Certain cell captive insurers have a large number of cell captive arrangements, but their internal resources are limited, and they cannot therefore exercise adequate oversight of the conduct of each cell owner. Ultimately, the Regulator notes that the insurer is responsible for ensuring that the cell captive arrangements and cell owners conduct themselves in a manner that consistently adheres to the standards of conduct expected of the insurer itself.

The cell captive conduct standards are awaiting finalization and may be expected later in 2021 or in 2022.

02

FinCrime

Financial crime is one of the largest systemic risks to the global economy, with devastating impacts on businesses and communities around the world. The impact of regulatory investigations and fines over the past 10 years on the financial services industry has been huge, both from a cost and operational perspective. These costs have included the execution of large-scale investigation and remediation projects. Firms not faced with regulatory inquiries have, nevertheless, incurred increased costs through reinforcing their compliance control frameworks to ensure that they stand up to regulatory scrutiny. In South Africa, there is likely to be an increase in fines and penalties imposed by the respective regulators for inadequate Risk Management Compliance Programs (RMCPs) and related controls as soon as inspections resume to normal post the COVID-19 pandemic.

The South African financial crime regulator, the Financial Intelligence Centre (FIC), models the country's anti money laundering and counter terrorism financing (AML/CFT) regime on the guidance set out by the Financial Action Task Force (FATF), the international AML standards setting body. As a FATF member country, South Africa is routinely inspected by the FATF and needs to demonstrate adherence to the FATF guidance and recommendations. To this end, the Financial Intelligence Centre Act (FIC Act) imposes various obligations on accountable institutions related to identification and verification of clients, transaction monitoring and reporting and record keeping, among others.

The FIC Act was amended in 2017 to improve the protection of the integrity of South Africa's financial system and strengthen its ability to prevent and punish financial crimes like money laundering, illicit capital flows, tax evasion, corruption, bribery and financing of terrorism. The FIC Amendment Act introduced various new requirements such as:

- Risk-based approach
- Customer Due Diligence (CDD) measures
- Record keeping requirements
- Risk Management and Compliance Programme
- Targeted financial sanctions

In order to give effect to these new requirements, institutions are required to implement enhanced governance and training as well as ensure that they appoint a compliance officer responsible for oversight of FIC Act compliance. As a result of the new requirements and risk-based approach, financial crime compliance spending has reached unprecedented levels trying to adopt automation, machine learning and AI into their process to increase efficiency and effectiveness. We note, however, that compliance processes are still dominated by high levels of manual, repetitive, data-intensive tasks that are not only inefficient, but are failing to disrupt fraud and financial crime. Furthermore, at the same time, new technologies, including cryptocurrencies, blockchain and open banking create new risks. Firms also have an obligation to comply with local data privacy legislation and/or regulations (e.g. the General Data Protection Regulation ("GDPR") and the Protection of Personal Information Act ("POPIA") as part of the money laundering and terrorist financing risk management system. South African financial institutions will need to play a balancing act to ensure satisfactory compliance with the relevant legislation while also keeping an eye on their bottom line.

Currently, cross border transactions are a focus of the Prudential Authority as well as the Financial Intelligence Centre. The regulators recently published a draft joint communication paper which sets out the requirements for instances when institutions process electronic fund transfer (EFT) transactions, both domestically and cross-border. The draft paper indicates in what circumstances institutions needs to report cross-border transactions, what minimum information needs to be requested before undertaking or accepting an EFT, what information should be included as part of the transaction and the circumstances for refusing or suspending a transaction. The document was published for consultation purposes and comments were received from the relevant industries. The paper is currently in the process of being finalised by the Prudential Authority and a final version is expected shortly.

03

Conduct of Financial Institutions (COFI)

COFI is intended to streamline the conduct requirements for financial institutions, which are currently found across a number of financial sector laws. This will result in a strong, effective and consistent market conduct legislative framework for all institutions, which undertake financial activities.

The second draft of the COFI Bill was published together with a Response Document that explains the key changes made to the first draft of the Bill, in response to industry comments and engagements held. Some of the key changes made between the first and second drafts of the COFI Bill include the following:

- Application of the COFI Bill in relation to existing legislation
- Approach to licensing
- Focusing transformation to tangible targets
- Approach to medical schemes sector
- Application to the non-retail market

The COFI Bill is expected to be enacted in 2022 and is expected to lead to further enhancement and embedding of conduct considerations in insurance organisations.

04

Micro Insurance

A major challenge in South Africa is financial inclusion, or the access to affordable and appropriate financial services by the financially vulnerable demographic of society.

In order to address the low penetration levels of insurance products among low-income earners, National Treasury issued a discussion paper in 2008 which ultimately culminated in the introduction of micro insurance via the Insurance Act, 18 of 2017.

In order to provide micro insurance, institutions need to apply for a specific license from the Prudential Authority. Micro insurance policies are limited to R100 000 for life insurance and R300 000 for non-life insurance. The micro insurance and funeral policies sold under this license must have a contract term not exceeding 12 months and may only provide risk benefits with no surrender value or investment elements. This type of insurance is governed by the same legislation as traditional insurance with specific product standards to be considered when products are developed. Micro insurance will also be subjected to annual audits and will have to submit audited annual returns and unaudited quarterly returns to the Prudential Authority.

In countries such as South Africa, where a large segment of the population cannot afford traditional insurance products, insurers who offer micro insurance have a significant market to tap into. Additionally, if microinsurers are innovative in their approach and use mobile technology to reach their customers and deliver their products, they will grab the attention of those customers who traditional insurers cannot reach.

While profitability is a major driver of insurers, environmental, social and governance factors are also becoming a focal topic globally. The social responsibility aspect ties in directly with the focus on financial inclusion, especially on the African continent. By providing affordable insurance products to people who really need it, insurers are making a positive contribution to society.

Our detailed Thought Leadership provides an in-depth analysis of Micro Insurance.

05

IFRS17

IFRS17 is the new accounting standard for insurance contracts and will be going live on 1 January 2023, with a parallel run during 2022. Compliance with IFRS is set out in the Companies Act of South Africa and is also a requirement of the JSE Listings Requirements.

The primary impact of the standard will be felt in the valuation and financial reporting teams, with secondary impacts on technology and operational teams in order to meet the underlying data and system requirements.

Firms that have not initiated their IFRS17 programmes should commence education campaigns, and compile project plans as soon as possible. In order to comply with the requirements of the standard, it will be necessary for firms to establish the:

- Required policies and methodologies
- Data, systems and processes
- Reporting structures

It will be necessary to acquire the relevant skills and systems, particularly subledger, to support these requirements will be acquiring the necessary skills and systems, particularly subledger to support the IFRS17 reporting requirements.

Firms are able to voluntarily move to IFRS17 before 2023. The formal parallel run period will commence in 2022 where IFRS4 and IFRS17 will be viewed in parallel.

Non-compliance will have possible ramifications from a listing perspective as well as compliance with the reporting in respect of the requirements of the Companies Act. Whilst not currently in place it is likely the Prudential Authority, who is currently taking a keen interest in Insurance Companies' progress with IFRS17, will also enforce compliance with IFRS17.

06

Recovery Planning

Recovery and Resolution Planning is anticipated to be a focus of the Prudential Authority going forward to ensure operational sustainability of the financial system, in particularly as a result of COVID-19 and the current state of the economy.

While the banks have already implemented Recovery Plans as a result of the Directive on Minimum requirements for the recovery plans of banks, controlling companies and branches of foreign institutions that was published in 2015 (D1/2015), this is yet to be enforced on insurance organizations.

As can be derived from the name, Recovery and Resolution Planning (RRP) consists of two components:

- Recovery Plan: aims to reduce the likelihood of failure, and
- Resolution Plan: aims to reduce the impact in the event of failure.

In contrast to the European approach to RRP where financial institutions are responsible for both, the South African regulator develops and owns the Resolution Plans, whereas the Recovery Plans are developed and owned by each respective financial institution. Resolution Plans are established by the regulator for Systemically Important Financial Institutions (SIFIs) as they pose a higher systemic risk to the financial system.

With "Twin Peaks" or the" Financial Sector Regulation Act" coming into effect in April 2018, the regulatory landscape in South Africa has shifted, bringing together the banking and insurance regulators.

As a result, the principles in certain of the directives for banks may equally be relevant for insurers. The regulator is on a journey to harmonize those requirements across all supervised financial institutions in the future.

In October 2020, the SARB's Financial Stability Department published a discussion paper on the methodology to determine which insurers are systemically important within the South African context. This document was open for comment until December 2020. By applying this methodology, insurers will be designated as SIFIs.

The benefits of establishing a Recovery Plan include aiding the insurer in understanding its own risks from severe stress scenarios and to be prepared to effectively respond in times of crisis, by thoroughly analyzing recovery options in advance thereof and developing practical action plans to implement these. This enables risk and crisis management to be strategic, rather than reactive.

Given the regulatory agenda explained above, it is sensible for insurers to include this in their planning and given the benefits of Recovery Planning, this can lead to a competitive advantage. As such, we see insurance groups in the market starting to prioritize the development of their Recovery Plans.

07

Financial Conglomerate Supervision

Per the Regulators Regulatory Strategy roadmap, regulations related to the supervision of financial conglomerates is expected to be promulgated to obtain a holistic view of group-wide activities, intragroup transactions and large exposures which, among other things, may not be captured under Level 2 supervision (consolidated supervision). The regulations are anticipated to be formalized in the latter half of 2022.

08

Third Party Risk Management (TPRM)

There are several types of risks that organizations using third parties need to consider. These include:

- Strategic,
- Operational,
- Financial,
- Geopolitical,
- Regulatory,
- Digital,
- Cyber and Privacy,
- Resiliency, and
- Reputational.

The level of exposure to these upside, downside and outside risks is based on how organizations are using the third parties.

For example, third parties may have a significant impact to an organization's operational risks if a third party provides a critical product or service to the organization.

- What happens if a third party is unable to perform according to their service level agreement due to a disruption in service or a defect in their production line?
- If a natural disaster occurs, how does an organization manage business continuity and resiliency risk when third parties are providing the parts and supplies necessary to operate business as usual?
- What happens if a third party fails to adhere to regulatory and legal requirements and is subject to severe legal penalties and fines?

To address the associated risks that third parties pose, organizations need to have a robust TPRM capability in place that builds trust by design. Without a consistent and comprehensive TPRM framework, organizations risk reputational damage, incomplete monitoring efforts and increased costs. TPRM provides a better understanding of third party relationships by tracking the metrics related to third party controls, performance and activities. By effectively managing third parties on an ongoing basis, organizations can evaluate whether the risks outweigh the costs of doing business with third parties.

TPRM activities should be embedded into every phase of the third-party management life cycle. Specifically, organizations will want to consider undertaking the following actions:

- Instill oversight and Governance - Establish a robust governance structure with engagement from the board and C-Suite so that sound risk management practices are embedded into the organization's culture, by setting the tone at the top.
- Get a full view of your third party inventory - Identify, categorize and assess your existing third party population to effectively manage your third-party inventory.
- Establish a risk-based approach and models - Adopt risk models according to your organization's risk appetite and culture. Determine the level of risk your organization is willing to take and derive the requirements for the respective categories of third parties accordingly.
- Implement policies and standards - These should outline the purpose and phases of the TPRM framework and define the roles and responsibilities of accountable stakeholders.
- Establish and execute TPRM processes - These should be cascaded into each phase of the third-party risk management life cycle.
- Harness emerging technology to improve risk mitigation outcomes - Use technology to automate processes, analyze data and report metrics to improve decision-making and understand the operational effectiveness of the TPRM function.

Within most insurers, TPRM is currently still relatively immature, compared to banks, and cyber / IT security and BCM related to third parties are key concerns for insurance CROs. Similarly, the 10th Annual EY/IIF Global Bank Risk Management Survey revealed that the key risks related to third parties that banks are concerned about are cyber / information security, business continuity management and reputational risk.

09

Privacy

Organizations have been granted a grace period of one year to normalize and implement the requirements of the law within their risk and compliance frameworks and must be able to demonstrate compliance by 1 July 2021.

Having recognized the need to regulate the use of personal information within South Africa, the Protection of Personal Information Act (POPIA) was enacted, with the bulk of sections commencing on 1 July 2020, effectively ushering South Africa based organisation into the new era of data privacy.

What are the next steps?

1. Register your Information Officer and Deputy Information Officer(s) with the Information Regulator. As per a media statement issued by the Information Regulator on 24 March 2021, the registration of Information Officers and Deputy Information Officers will commence on 1 May 2021. The registration process will be an online one as per the statement.

2. Establish a robust privacy framework to demonstrate compliance to the requirements of POPIA. Organisations will need to ensure that the framework meets the expectations of the Information Regulator. This will imply answering the following key questions:
   - The Deputy Information Officer must report to the highest management office within an organization. Who should be appointed as the Deputy Information Officer and where should this function sit to meet this requirement?
   - Are the duties and responsibilities of your Deputy Information Officer in conflict with other duties assigned to him or her?
   - Are you considering data protection issues as part of the design and implementation of systems, services, products and business practices?
   - Do you have privacy notices/statements at each point of collection of personal information?
   - Do you have a functional process to identify, assess and address data privacy risks in line with the requirements of POPIA? How integrated is this process with your overall Enterprise Risk Management (ERM) framework?
   - Do you have a clear picture of what types of information you hold, for what reasons they are processed and where they are stored?
   - Have you developed and communicated a set of policies and procedures to support the privacy framework?
   - Do you know within how many days you are required to respond to a data subject request? Have you assessed whether your organisation is prepared to respect this timeframe?
   - Would your employees recognise a personal information breach when they saw one? Would they ignore it? Would they know what to do about it?
   - Do you have appropriate skills and resources to support the privacy framework?
   - Do you have sufficient overview of the privacy posture of your departments and service lines?
   - Are you disposing of personal information when the retention period has lapsed? Have maximum retention periods been defined and personal information tagged for disposal accordingly?
   - Do you know whether your service providers are processing your data as per your expectation?
   - Are you sure that you are processing your clients' and employees' data as per their expectation?
   - Are you ready to demonstrate proof of compliance to the Information Regulator as from 1 July 2021?

https://www.ey.com/en_za/cybersecurity

https://assets.ey.com/content/dam/ey-sites/ey-com/en_za/generic/ey-popia-report-2020.pdf

10

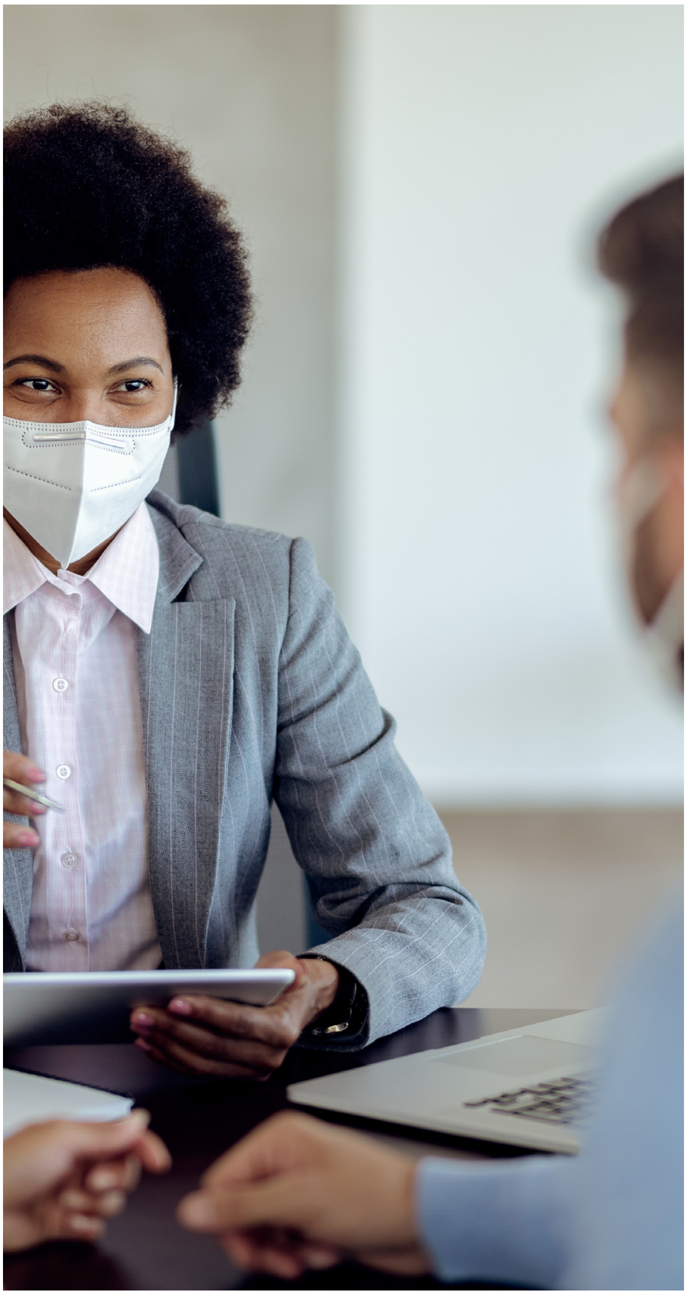
Cloud computing/Offshoring of Data

The financial services industry has faced many challenges in recent years in respect of maintaining the integrity of the data they control. There has been numerous data breaches and the implications have been severe. Added to this is the imminent promulgation of the Protection of Personal Information Act (POPIA), which takes effect in July 2021.

Cloud computing and offshoring of data is therefore something that has captured the regulators attention. To address this, the SARB has published Directive 3 of 2018, read with Guidance Note 5 of 2018, which sets out the minimum requirements under which Banks may use cloud computing or offshoring of data. Banks are required to have in place a formally defined and board approved data strategy and data governance framework.

While this Directive and Guidance Note are currently not legally binding on insurers, it is prudent to note that the PA may consider the principles contained therein to be equally applicable to other supervised financial institutions. The PA is in the process of harmonizing various regulatory instruments in order for those to be applicable across all supervised financial institutions.

It is therefore imperative for Insurers to start focusing on this area to ensure that they have the necessary governance structures and frameworks in place that will enable them to comply with these requirements once they become applicable.



11

Global Trends

EY 2021 Global Insurance Outlook Report

This report highlights the current state of the insurance industry and also sets out the strategic steps insurers need to take in order to navigate the next 18-24 months. COVID-19 has been a major disruptor to the insurance industry and more disruption as well as evolution of financial organizations is expected. It is therefore necessary that insurers take proactive steps to prepare for this. To this end, there are 3 strategic imperatives insurers should follow in order to create value for themselves as well as society as a whole:

1. Redefine and refine purpose in setting the strategic direction

Insurers need to determine their purpose and understand how to use it to create long-term value for their organization. In order to do this, insurers should:

- "Stress-test" their existing purpose considering the pandemic, social issue and climate change;
- Develop targeted product offerings to address savings and/or protection gaps for specific customer segments; and
- Define metrics to guide capital allocation and monitor the impact of purpose-driven policies and actions.

2. Transform the business to be more agile, digital and customer-centric

Every facet of the insurers business should be designed around deep insights into customers needs. By making their operations more agile and embedding stronger digital capabilities, insurers can meet customer expectations for speed and personalization. To achieve this, insurers are advised to:

- Simplify application and purchase processes while rapidly increasing the intake of third-party data to enhance underwriting, marketing and policy administration;
- Tier and tailor products and solutions for specific customer needs and different price points; and
- Create digital services, platforms and ecosystems that lead to stronger customer engagement and generate new demand.

3. Create value by optimizing cost management and capital allocation

The COVID-19 pandemic made a large negative impact on the balance sheet of insurers. In order to recover the gains made before the pandemic, insurers should consider options such as automation, divestment, restructuring and outsourcing. Instead of cost-cutting, insurers should manage a strategic cost agenda that is based on lean and agile operations with a flexible cost structure that allows the business to easily scale up or down as the business expands or contracts. A few ways to achieve this includes:

- Expand cloud adoption exponentially in the next 24 months;
- Refine their alternative capital strategy and identify plans for targeted growth investments; and
- Reassess productivity considering hybrid working models, increased automation and shifts in workplace composition.

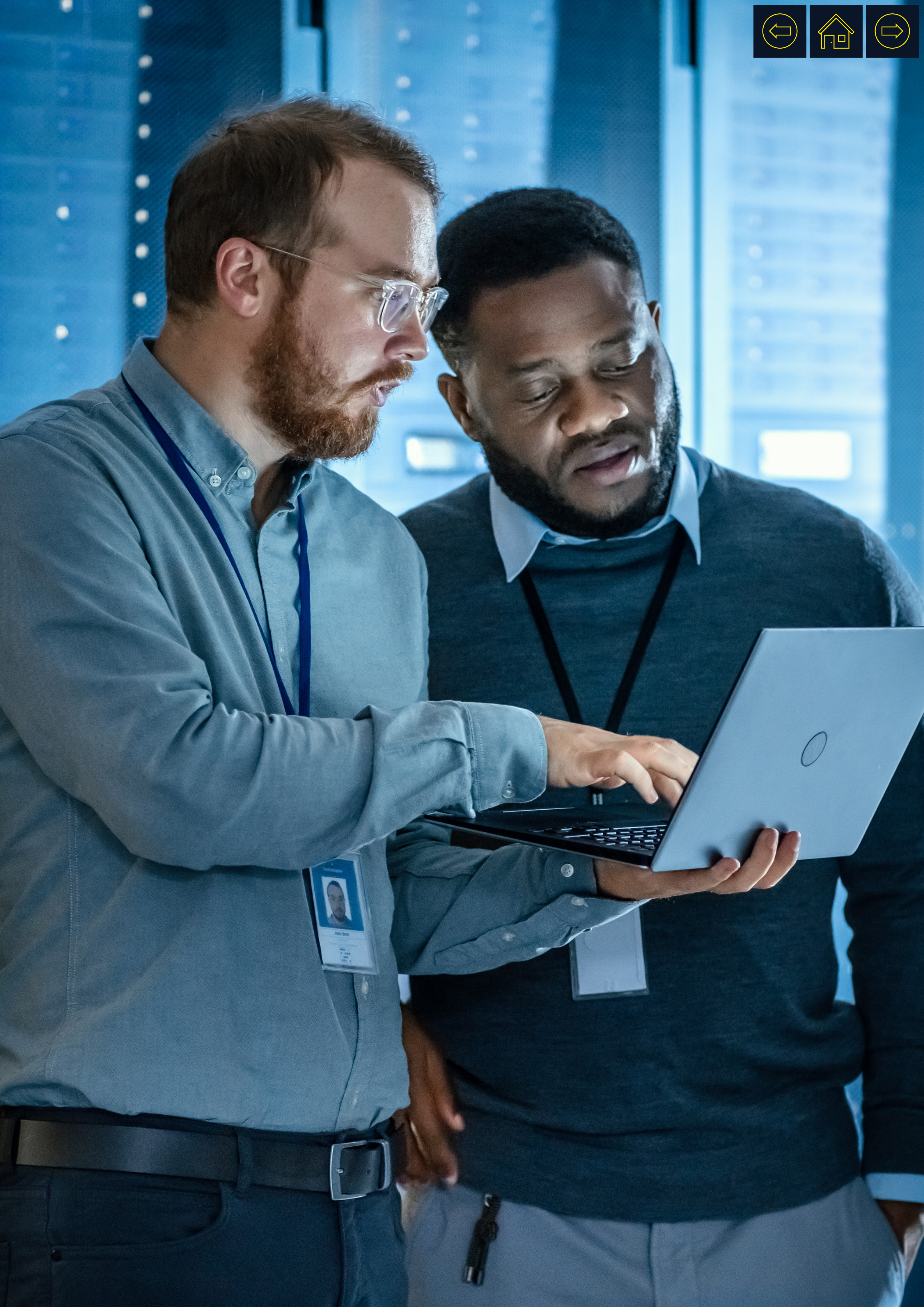
Product Innovation

The COVID-19 pandemic has had a massive financial impact on insurance consumers. Surveys conducted have highlighted how the pandemic has led to a shift in consumer priorities, behaviors and insurance needs. Across the world, during the early stages of the pandemic, there was a rapid shift to remote working. Offices stood empty and cars were no longer being driven as much as usual.

Home offices became the new norm. Fast forward to a year later and many companies have still not returned to the office. Some of those that have returned still retained an element of remote work. And consumers realized that paying for insurance they weren't using wasn't practical any longer.

The heightened financial anxiety experienced by consumers led to them seeking cost effective insurance alternatives and policies with lower premiums. The insurance industry provided relief in the form of payment holidays in order to retain their clients but the closure of companies, reduced staff needs, and salary cuts meant that many insurance consumers simply cancelled their insurance policies. Insurance companies therefore needed to be innovative in their approach and understanding of consumer needs. This has resulted in various companies offering usage-based insurance e.g. consumers who are now working from home have the option to insure their vehicles based on how much those vehicles are actually used. Other types of insurance made more popular as a result of remote working during the pandemic are home protection insurance and cyber fraud insurance.

In order to meet the evolving concerns and needs of consumers, insurers must reevaluate their offerings and overall value proposition for both existing and prospective customers. This may be easier said than done as a survey conducted in December 2020 indicated that product and proposition development was the function predicted to face the greatest challenge in adapting to change. The COVID-19 pandemic proved to be the ultimate test of insurers' resilience and ability to adapt and the successes or failures in this industry will be evident as the world continues to navigate the new normal.



ESG

Sustainability will return to centre stage in 2021. An immediate boost is the new Biden administration's decision to re-engage in global climate talks, with both Washington and Brussels talking about linking trade and climate agendas.

This is accompanied by renewed worldwide regulatory pressure for adoption of sustainable finance frameworks and growing support for the agenda from large international banks, investors and corporates. The foundation of climate risk regulation must now be put in place via a taxonomy that can serve as a list of "green" economic activities and a basis for a series of disclosure requirements for corporates, financial market participants and financial products.[1]

The sustainability agenda is now a leading strategic priority for many insurers. This extends beyond their products and services, investment decisions and risk management. It increasingly includes corporate social responsibility, with insurers becoming a leading voice on climate risk and mitigation in particular.

ESG priorities are focused on sustainability, corporate responsibility and their material financial impact on an organization's immediate, medium-term and long-term value. The strategic priorities and objectives of the three ESG pillars include:

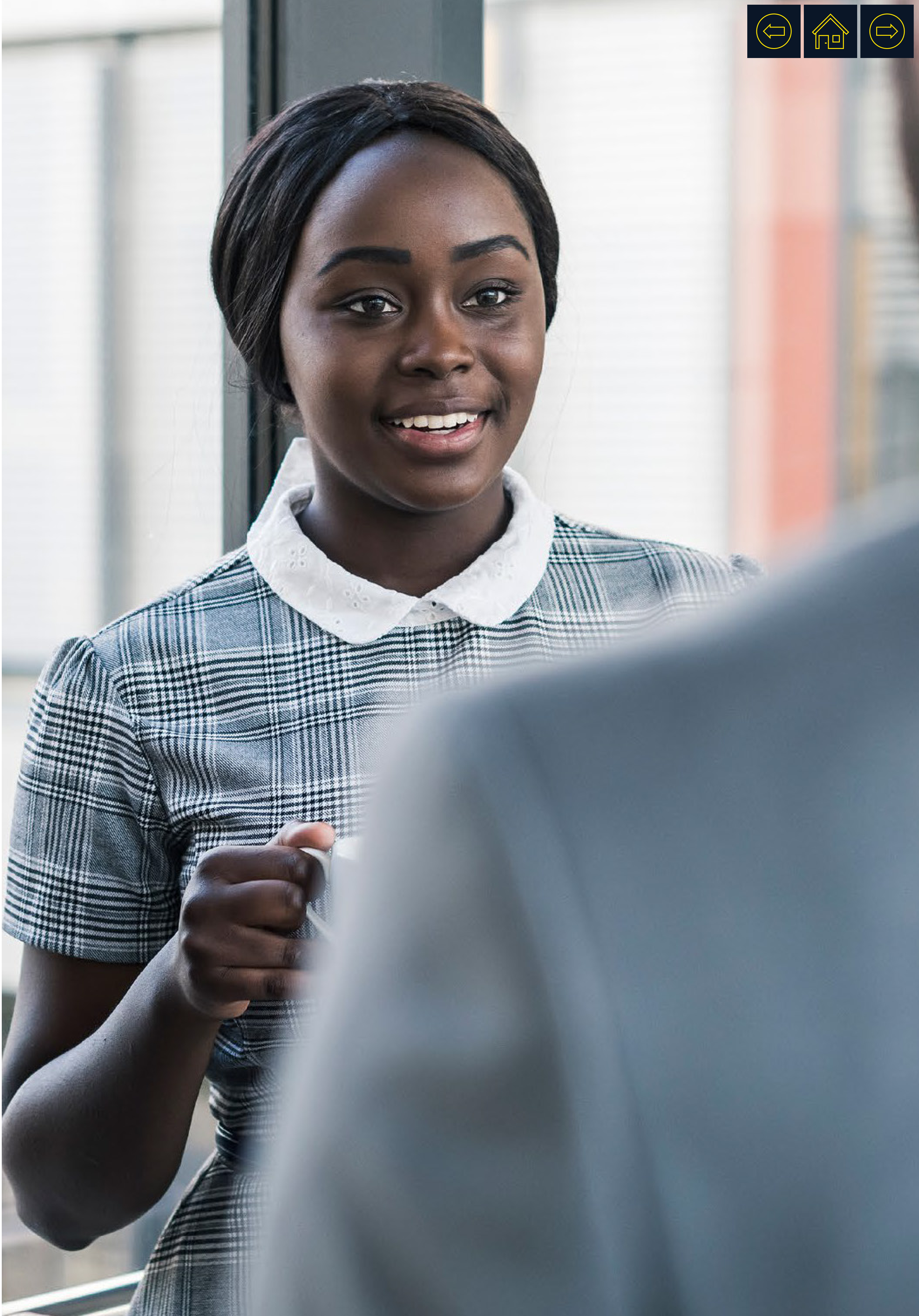
- Environmental: the impact of climate change on an organization's business model
- Social: the value that businesses create that potentially impacts investors, employees, customers and communities
- Governance: the system by which all core business activities are directed, controlled and monitored as it is critical to create long term value

How to strengthen board oversight of ESG
COVID-19 disruptions, accelerating "new normal" transformation, stakeholder capitalism and concerning climate change risks have elevated ESG to become a strategic business imperative. Boards can strengthen ESG oversight to build company resilience and unlock long-term value creation through the consideration of five actions:

1. Address heightened expectations of investors and stakeholders
2. Understand the ESG ecosystem and stakeholders' expectations
3. Guide ESG strategy development
4. Support the integration of ESG into enterprise risk management (ERM)
5. Communicate the ESG story

Click here

[1] *https://intranet.ey.com/sites/fso-content/newsviews/460400/210408_how-insurers-are-faring-on-sustainable-finance*



12

How can EY Help?

EY has a dedicated Financial Services Consulting practice, which includes Risk Management, Technology, Process and People. This gives us deep industry knowledge in all aspects of the financial services industry, allowing us to tailor integrated solutions to our clients' specific needs.

Our Financial Services Risk Management (FSRM) consulting practice, has experience with financial services companies and regulators in various jurisdictions, and comprises of a variety of skills across the insurance and banking sectors. We combine local regulatory and legislative knowledge with best practices in global prudential regulation as well as governance, risk and compliance (GRC). Through our fully integrated global Prudential, GRC and Actuarial networks, we ensure that we are at the forefront of global regulatory developments. We leverage this to approach compliance and risk management not only from a regulatory perspective, but also from a strategic perspective.

Market Conduct

The FSRM team can assist in helping financial services organisations design their interactions with customers and counterparties, to deliver fair outcomes and market integrity, and effectively manage associated regulatory, reputational and strategic risks. We can do this by:

- Assisting our clients with the design and development of market conduct and organisational frameworks, and assist in implementation thereof, and
- Performing gap analyses against the regulatory requirements and benchmarking compared to local and global practice of existing market conduct frameworks.

Governance, Enterprise Risk and Compliance

- Within the GRC space, our FSRM team can assist in:
- Reviewing Governance Policy and Control Adequacy,
- Assessing the maturity of Risk / ERM and Compliance Functions (including benchmarking to best practice),
- Developing or assessing 3rd Party Risk and Binder Risk Management Frameworks,
- Designing, implementing or enhancing Credit Risk Frameworks,
- Establishing ESG governance frameworks and design disclosure,
- Developing, implementing or enhancing Model Risk Management,
- Setting up or reviewing Recovery and Resolution Planning,
- Assisting in preparing for the requirements under the Financial Conglomerate Supervision/Regulation,
- Assisting in selecting GRC solutions and implementing these, and
- Establishing and management of Regulatory Inventories and risk controls.

Prudential Risk

The services offered to banks and insurers include:

- Reviewing Regulatory Capital Requirements (BA Returns and Quantitative Returns),
- Reviewing or performing ICAAP/ORSA,
- Assisting in Capital and Balance Sheet Optimisation / Management,
- Developing Economic Capital models,
- Performing reviews of Pillar 3 Requirements for Banks,
- Supporting in IBOR/JIBAR transition implications and preparation,
- Optimisation of overall financial resources

EY can assist with defining the prudential regulatory framework and the pro-active strategic response to mitigate the implications of these regulations on key financial indicators.

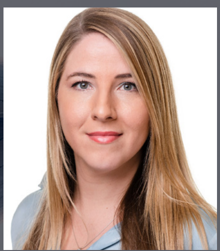
EY's global regulatory network leverages regulatory knowledge on an international scale. We can support our clients in understanding and addressing the most critical financial and compliance impacts for their business as a result of regulatory change and help them to implement solutions on a cross-border basis to support compliance wherever they operate.

In today's environment of heightened and evolving regulation and structural changes, our professionals can work side by side with our clients to interpret new rules as they are issued. Through this collaboration, any compliance and operational changes that are required can be identified quickly and processes can be established to implement them efficiently.

Contacts

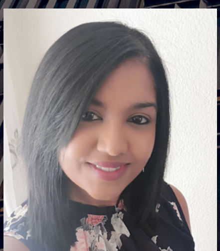
Trevor Rorbye
Partner
Africa - Insurance Sector Leader
trevor.rorbye@za.ey.com

Jaco Louw
Africa FS Risk Leader,
Africa IFRS17 Lead
Jaco.Louw@ey.za.com



Idelia Hoberg
Associate Partner
Financial Services Risk
idelia.hoberg@za.ey.com

Threshern Naidoo
Senior Manager
Financial Services Risk
threshern.naidoo@za.ey.com



Divinia Naidu
Manager
Financial Services Risk
divinia.naidu@za.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

Creative Services ref. 6991. Artwork by J. Aricksamy.

ED None

ey.com