KPMG

Ten key regulatory challenges of 2023

Strengthening the links

kpmg.co.za

Introduction

On behalf of KPMG's Africa Regulatory Centre of Excellence I am delighted to present our ten key regulatory challenges of 2023. This year we focus on strengthening the links between the various regulatory challenges facing the financial services sector for maximum strategic advantage.

I challenge you to consider where you can enhance and reinforce your regulatory framework using this strategy. This will provide a solid base built on learnings from the past, combined with the agility to respond to new developments with minimal disruption to business. Importantly, this approach will put you in a position to demonstrate compliance to our regulators.

1. **Economic and Political**
2. **Climate and Sustainability**
3. **Transparency and Reporting**
4. **Data and Cybersecurity**
5. **Technology and Resilience**
6. **Credit and Capital**
7. **Scrutiny and Divergence**
8. **Fraud and Financial Crime**
9. **Fairness and Inclusion**
10. **Risk and Governance**

We encourage you to reach out to us to learn more about the issues and actions highlighted in the following pages or to discuss your firm's unique challenges.

Michelle Dubois

Senior Manager
Regulatory Centre of Excellence Lead
T: +27 60 997 4512
E: michelle.dubois@kpmg.co.za

Ten key regulatory challenges of 2023

1. Economic and Political
2. Climate and Sustainability
3. Transparency and Reporting
4. Data and Cybersecurity
5. Technology and Resilience
6. Credit and Capital
7. Scrutiny and Divergence
8. Fraud and Financial Crime
9. Fairness and Inclusion
10. Risk and Governance

1 Economic and Political

1 Economic and Political

The conundrum of knowns and unknowns

Economic and political risk, also known as geopolitical risk, is signified throughout former US Secretary of Defense Donald Rumsfeld's matrix of "known knowns, known unknowns, unknown knowns and unknown unknowns"[1]. These types of risk often originate in the minds of powerful individuals and therefore it is generally impossible to foresee new geopolitical risks ("unknown unknowns") that may develop. Even when considering existing geopolitical risks ("known unknowns") it is just as challenging trying to quantify the likelihoods of certain outcomes materializing although we can usually be clear that the economic implications of those outcomes will have a significant impact.

The most relevant example of a recent geopolitical event that has had a large impact on the global economy was Russia's invasion of Ukraine. Even though Russian troops and armaments had amassed on the Russia Ukraine border towards the end of 2021, most analysts at that time predicted that based on the costs and benefits of a potential invasion of Ukraine, Russia was unlikely to invade. The Russian invasion of Ukraine was therefore accepted by most people as a low probability but potentially high impact event and as it became a reality, those resulting impacts became known. Due to the significance of both Russia and Ukraine in global energy and food markets, the invasion resulted in large price increases as the fighting itself. Retaliatory sanctions and political maneuvering interfered with the supply of energy, food and related markets and resulted in the prices of these goods accelerating through much of 2022. As a result, what was predicted to be a year in which the global economy returned to its post-COVID-19 pandemic potential growth, turned out to be a succession of inflationary increases followed by increases in interest rates and the subsequent downgrading of economic growth rates.

By the end of 2022 the general unknown in financial markets was the degree to which central banks were prepared to increase interest rates to force a reduction in inflation to more sustainable long-term levels. If central banks did too little in this regard, economies could experience higher levels of income and wealth-eroding inflation to persist for an extended period of time. By contrast, if central banks tightened monetary policy by too much, then many economies across the globe would experience recessionary conditions or contractions in economic activity due to the resulting restricted consumer and investment expenditure. The weight of opinion was generally in support of the latter outcome with market analysts expecting a mild recession to result in the United States, a deeper recession to result in Europe, a recession in the United Kingdom and similar forecasts of recession for many other economies around the world in 2023, including for South Africa.

Looking towards the future there are a number of "known unknowns" to consider, all of which have the potential of resulting in high impacts on global economic conditions and by implication, on global and local financial markets.

The first of these concerns is the next phase of Russia's invasion of Ukraine. There are a number of potential scenarios to consider of which we will cover four below.

- The first is that Russian President Vladimir Putin is ousted during 2023 due to internal pressure created by the inability to realise Russia's stated goals put forward as a result of the invasion of Ukraine, as well as the global ostracization and international costs imposed on Russia. Although a low probability event, the result could be an agreement to end hostilities and a normalization of energy and food markets. This would lead to a reduction in global inflation and facilitate a faster return to lower interest rates, thereby increasing global economic growth prospects and boosting financial markets. Such an outcome would potentially allow the South African Reserve Bank (SARB)[2] to reduce interest rates towards the end of 2023 based on expected reduction in food and energy inflation. This would also assist in increasing growth expectations both due to an expected increase in domestic economic activity, but also assisted by increased trade with the rest of the world.

[1] Former U.S. Secretary of Defense Donald Rumsfeld at a press conference in 2002

[2] South African Reserve Bank

1

- The second potential scenario is that the increased pressure experienced by President Vladimir Putin due to the internal pressure created by the inability to win the war and realise Russia's stated goals as well as the global costs imposed on Russia result in the selective utilization of tactical nuclear weapons in Ukraine. This scenario, although possible, is also allocated a small probability of occurring, but the implications thereof would be deep and far reaching. NATO[3] would need to intervene and the conflict would be escalated to include many more nations and cover a larger geographical region. Such a situation could last for an extended period of time and destruction to global markets and prices would be similarly impacted leading to extended recessions and consequential contractions in financial markets. South Africa could expect a marked depreciation in its exchange rate as capital seeks safe havens. Weaker global trade and growth conditions be combined with high inflation and interest rates could easily lead to stagflation which may last for quite some time.

- A third scenario would be that the previously mentioned costs of the conflict on Russia would lead to an agreement between Russia and Ukraine to end the war, with Russia vacating Ukrainian territory potentially also including the Crimean Peninsula. Although also a low probability event given the potential implications of such an option for President Vladimir Putin, the result would once again be the normalization of energy and food markets leading to a rapid reduction of global inflation and more positive global economic growth prospects and a boost to financial markets. South Africa could expect increased growth based on lower interest rates that would be possible under a more benign inflationary environment, as well as appreciation in its exchange rate as global demand for commodities accelerates and investors are prepared to take more risk and invest in emerging and developing markets.

- The final scenario considered, and potentially the most likely scenario, is that the conflict in Ukraine continues through 2023 with an expected Russian spring offensive countered by greater international assistance in terms of the additional supply of weaponry and ammunition for Ukraine. Such an outcome would keep energy and food markets under continued pressure requiring higher interest rates for longer in order to bring inflation down to a more sustainable level potentially only by 2024. As a result, global growth expectations would remain relatively weak and financial markets would remain suppressed with volatility remaining elevated.

The other potential geopolitical events all include China as a protagonist due to the rise of China as an ever more powerful global force. The first scenario concerns the relationship between China and the United States of America.

- The world's two largest countries as measured by economic power have been involved in a number of battles. From trade and exchange rate disputes following years of globalization-induced exchange, to issues of human rights sovereignty and intellectual property, as well as possible future competition based on military might and even exploration and commercialization of space. The relationship is characterised by a lack of trust in the intentions of the other based on each nation's differing view of the world, with China and its communist system being seen as a threat to western freedom and liberty, while the US is perceived to be a bully trying to prevent the rise of China as the pre-eminent global power. The recent incidents where a Chinese balloon, thought by the US to have been a spy balloon, was shot down over Montana only confirmed to most Americans that China remains a threat. The relationship between America and China remains at the forefront of geopolitical events and has the potential implication of greatly improving or diminishing the welfare of all nations around the world over the years to come.

The second of these concerns a potential conflict between China and Taiwan around the sovereignty of Taiwan.

- The probability of shots being fired across the Taiwan strait or any direct conflict occurring remain small for 2023. The potential implications of this would be far reaching and would also impact the global economy and perhaps change the current international relationships permanently. What appears to be more likely is the ongoing activity of China in the South China sea as well as trade and other political avenues in order to attempt to calibrate the limits to which it can assert itself on Taiwan before initiating a formal US and potentially a NATO response. It is clear that China sees Taiwan, or officially the Republic of China, as part of mainland China as it is prepared to take a long-term view to secure this.

[3] North Atlantic Treaty Organisation

1

The final of these closely watched geopolitical progressions relates to the relationship between China and Russia.

- At the time of writing, Russia and China were celebrating the second anniversary of their no-limits friendship, which refers to a statement made by Chinese President Xi Jinping days before President Vladimir Putin's invasion of the Ukraine. The past relationship between these two countries has not always been as congenial with past wars and conflicts, where Russia, under the last enfeebled imperial dynasty, captured 1.5 million square kilometers of Chinese territory. The inconsistent history of their relationship adds interest around the current friendship based more around geopolitics and trade. It should therefore be no surprise that China has not sided with most other countries in totally condemning Russia's invasion of the Ukraine and consequent treatment of Russia as a pariah. It appears in this regard that relationships are established and friendships are maintained where China thinks it will be economically and politically beneficial to do so, irrespective of what has happened in the past. The progression of the relationship between China and Russia will remain important over the years to come and the direct or indirect impact of this relationship has the potential to be severely disruptive to the global and economic landscape.

On a domestic level two recent events may potentially indicate a shift in South Africa's relationships with the rest of the world, and particularly from the traditional West and more towards China and Russia. The first of these was the January 2023 visit of Russian Foreign Minister Sergei Lavrov to South Africa to renew cooperation between the two nations at a time when global relations with Russia are strained due to their invasion of Ukraine. The second concerned the joint naval exercises that took place with both Russia and China in February 2023. On the other hand, South Africa has conducted similar military exercises with the US, UK and France and the visit by Russia's Sergei Lavrov was closely followed by a visit by US Treasury Secretary Janet Yellen. Any changes in these relationships could have far reaching implications for South Africa. This includes reduced access to Western technology and defence and developmental assistance, given that Europe and the United States in particular make up our main trading partners in this regard.

Of similar importance and risk as South Africa's changing international relationships, will be the results of the 2024 general elections. The long-term performance of the ruling ANC government has been underwhelming and has led to a consistent decline in political support leading to speculation that they could potentially lose the majority at the 2024 general elections. Such an outcome would potentially lead to years of coalition rule which could result in a range of potential outcomes. There are mixed results concerning the effectiveness of coalitions to be able to work together to consistently serve the public at local level with competing interests and ongoing political battles often hindering service delivery, accountability and public administration. However, coalition politics and increased oversight may reduce the levels of corruption and mismanagement leading to more resources being available for public services and resulting in potentially greater impact being made on growth, employment and alleviation of poverty. The uncertainty of the outcome of the 2024 general elections is indicative of the risks faced for South Africa over the short-term, with a smaller probability of better governance resulting in improved political and economic outcomes contrasted against a larger probability of a continuation of the slowly deteriorating economic conditions.

As we enter 2023, the year in which we expect the population of India to surpass China signaling potentially the entrance of another powerful protagonist into the geopolitical arena, we will follow the scenarios set out above with interest, based on their potential impact on global power relationships and how these will impact our economy. Geopolitical events present both threats and opportunities to businesses as they develop. Financial services organisations should incorporate their understanding of how these risks could impact their businesses into their individual strategies.

Frank Blackmore

Lead Economist
Financial Risk Management
T: +27 73 672 6923
E: frank.blackmore@kpmg.co.za

1

The transition from Jibar[1] to ZARONIA[2]

The highly publicised irregularities relating to the production of interbank offered rates (IBORs) initiated a global regulatory response to reform major interest rate benchmarks. The use of the IBORs within financial markets has subsequently reduced substantially in favour of more robust, alternative reference rates (ARRs), namely, overnight reference rates (ONRRs) which are *near risk-free.*

South Africa has also embarked on the transition journey with the release of the consultative paper [SARB, 2018], prepared by the South African Reserve Bank (SARB), which detailed its initial proposal.

The SARB subsequently formed the Market Practitioners Group (MPG) in 2019 to manage the process of adoption and transition to the new interest rate dispensation. The SARB's MPG is a joint public and private sector body, comprising representatives from the SARB, the Financial Sector Conduct Authority (FSCA), and senior professionals from a variety of institutions from different market interest groups active in the domestic money market.

The traditional suite of benchmark rates in South Africa consisted of a set of Jibars (1-, 3-, 6-, 9- and 12-month). The 3-month Jibar rate is currently the most commonly used benchmark rate for interest rate derivative products denominated in South African rand (ZAR). Like the IBORs, Jibar lacks the primary market activity which puts it at risk of being not representative of the underlying market it is meant to measure.

Taking into account the recommended properties for a viable replacement reference rate, the MPG has designated the South African Overnight Index Average (ZARONIA) as the preferred successor rate to replace Jibar and SAFEX ON. The conceptual design of ZARONIA was rigorously tested, using real and genuine transactions data to ensure that it is reliable, robust and sufficiently stable.

The designation of ZARONIA as the preferred successor rate forms part of a larger transition roadmap which includes establishing a successor rate, adoption of the successor rate in both derivatives and cash markets, transitioning legacy contracts and eventual cessation of Jibar.

The SARB are basing their position on what they've observed in different jurisdictions and by interacting with different authorities. Their position is that a term rate is not the destination for all markets. The timing of the term rate becoming available is uncertain because of its dependence on building liquidity and depth in the Overnight Indexed Swap (OIS) market to make sure the rate aligns to International Organisation Of Securities Comission (IOSCO) principles; they will need to encourage transition in all other markets as this happens.

The UK authorities made it clear that their preference was for a market to adopt a broad-based transition to SONIA compounded in arrears, and the use of a term rate is limited. Similarly, ZARONIA compounded in arrears is expected to be the primary vehicle for the transition away from JIBAR. This is in line with international markets experience, as they found that the rate in arrears is more robust than the forward-looking rate. The cash market will want to use the same convention as their hedging activities to ensure cost efficient hedging. The arrears rate is applicable to multiple markets which allows users to access consistent and reliable costs of borrowing.

The authorities did not want to create the same situation as that which occurred with LIBOR, i.e., a introduce structural vulnerabilities by allowing the derivatives market to have several trillions of contracts referencing a rate that has comparatively small underlying transactions.

As most South African financial services organisations have been through their respective IBOR transition project for USD, GBP and EUR, replacing LIBOR rates with alternative reference rates such as SOFR, SONIA and ESTR, they must now prepare for their local transition from Jibar to ZARONIA. A critical success factor for this local transition will be to ensure that the insights from IBOR transition are leveraged for the benefit of the local transition, mobilising the experienced teams to adapt their learnings to the Jibar transition. Although the exact timelines are yet to be finalised, the transition must take place within the next two to three years to ensure that the South African market does not lose alignment with global markets.

Auguste Claude Nguetsop

Partner
Financial Risk Management
T: +27 82 719 2842
E: auguste.claude-nguetsop@kpmg.co.za

[1] Johannesburg Interbank Average Rate

[2] The South African Overnight Index Average (ZARONIA) is a benchmark that reflects the interest rate at which rand-denominated overnight wholesale funds are obtained by commercial banks.

2 Climate and Sustainability

2 Climate and Sustainability

The transition from vision and strategy to transformation and delivery

Financial services organisations are no longer driven to change by regulatory pressure alone. More and more, customers, investors and broader stakeholders are demanding that companies consider how their business impacts the world, their contribution to society and how they conduct themselves.

This trend has pushed financial institutions to set Environmental, Social and Governance (ESG) objectives and, in order to not be seen to be falling behind, to communicate to stakeholders about their ambitions, strategy and plans. The complexity of implementing these plans, however, poses quite a challenge. The time for vision and strategy development seems to be passing quickly, and financial services organisations now need to focus increasingly on transformation and delivery.

Successfully achieving wholesale transformation across the organisation and supply chain will depend on a few key success factors that organisations need to prioritise:

- Setting a clear strategy/vision for what is to be achieved

  Assessing maturity against peer market practice and performing impact analyses across the organisation are vital starting blocks to better understanding and detailing strategic ESG objectives, as well as identifying where the organisation finds itself on its ESG transformation journey.

- Align to corporate purpose, values and culture

  ESG objectives should be aligned to the organisation's purpose, values and culture and it is fundamental to set the tone from the top on the importance of achieving the ESG objectives within the appropriate timeframes.

- Enable cross-functional collaboration

  ESG is a pervasive challenge that touches every function within an organisation and will require cohesive delivery against the strategy. A holistic transformation pathway, illustrating the role that every function has to play in facilitating ESG change against each objective, can support an interconnected approach to transformation.

The three key phases of transition

There are three key phases of activities required to successfully drive transformation across the organisation. When setting the vision and strategy and assessing the current state it is important to also draft a communications plan and to execute on it. The next step, which is to design and prioritise, an end-to-end target operating model (TOM) must be designed in line with the corporate strategy. This will enable the establishment of an implementation plan and framework, as well as a governance structure. The business/investment case will be a fundamental component of this granular roadmap development process. In this phase it is key to cater for the prioritisation of activities and the enablement of cross-functional collaboration. Several functions can be seen emerging as enablers of wholesale transformation to deliver against a financial services firm's ESG goals:

- **Risk**

  Organisations are continuing to look for a more strategic approach to risk management whilst maintaining their independence as a second line of defence. ESG technology can be leveraged to enable risk owners to not only effectively manage key risks, but also to support firm-level risk strategy, for example through the use of real-time risk data and dashboards.

- **Finance**

  Finance plays a leading role in ESG reporting and data management programs. Finance sub-functions, such as the financial planning and analysis function, can connect ESG information, drive insights, and report on progress.

2

- **Operations**

  As the ESG reporting landscape continues to grow, greater reliance will be placed on the operations function to analyse and service sustainability products.

- **Compliance**

  The speed with which ESG compliance issues are evolving requires an equally dynamic and robust compliance function, underpinned by a strong ESG compliance framework to prevent fraud and misrepresentation.

- **Frontline business**

  Front office business is crucial to meet increasing demand for sustainable products, whilst maintaining integrity and transparency in the labelling and marketing of these products.

During the last of the three phases – implement, monitor and adapt - the TOM is implemented by outlining detailed activities for each function across a multi-year timeline, considering the established priorities. Given the quickly changing environment, as well as the absence of well-established market practices/benchmarks, it is fundamental to enable adaptability in the TOM and to implement constant monitoring. That way lessons learned can be taken into account during the transformation journey. This is also a reason why prioritisation is fundamental, focusing initially on a limited number of activities, as opposed to trying to achieve across the board transformation from the start, makes it possible to learn and avoid making similar mistakes across all activities. For example, in order to achieve net zero, a bank can initially focus on its activities in the energy sector and thanks to the experience gathered, tackle other impacted sectors more efficiently at a later stage.

Setting the pace for success

ESG transformation is a tightrope for financial services organisations. Go too fast and you create paper decarbonisation and will probably fail to help your communities and the real economy. Go too slow and you risk being accused of greenwashing or failing to take climate change and social and governance issues seriously. However, with the right approach and ESG transformation framework, financial services organisations can get it right and be key enablers in the fight for a more sustainable future.

Ulrich De Prins

Partner
Financial Risk Management
T: +27 60 976 7706
E: ulrich.deprins@kpmg.co.za

Charlotte De Koker

Associate Director
Sustainability Services
T: +27 64 758 2649
E: charlotte.dekoker@kpmg.co.za

3 Transparency and Reporting

3 Transparency and Reporting

Regulatory supervision and reporting for banks and insurers

The Prudential Authority, as a primary regulator for the prudential supervision of banks and insurers, takes a holistic approach to supervision. The emphasis is on ensuring that those in control of the organisation are "fit and proper" and that the organisation is adequately capitalised to sustain the nature and extent of all its operations.

As banks and insurers expand internationally, and diversify into non-core businesses, it becomes necessary to ensure that there is compliance with both international and local guidelines related to prudential supervision. The reporting and supervisory requirements of the Prudential Authority continue to evolve to meet these increasing levels of complexity.

Guiding principles of risk management

In its risk management approach to supervision, the Prudential Authority follows several guideline principles, namely:

- the Board of Directors (the board), not the supervisory authority, is primarily responsible for the management of the bank or insurer (which includes the relevant reporting to evidence as such);
- the benefits of regulation and supervision should exceed the costs related thereto;
- the supervisory process must be market driven and should meet international standards;
- the supervisory authority is committed to a consultative approach to supervision; and
- the supervisory authority is committed to consolidated supervision in line with international trends in supervision.

Financial regulation

A critical aspect of the Prudential Authority regulatory requirements is the framework of regulatory reporting which is required to be submitted on an ad hoc, monthly, quarterly, and annual basis. The reporting is based on the Basel Accord's as part of the Basel frameworks for banks. For insurers the local Insurance Act is modelled on the Solvency II regime as applied in Europe.

Monitoring framework

Prudential Authority

The Prudential Authority uses a combination of on–site and off–site supervision, embodying the principles of international best practice.

On-site supervision

The Prudential Authority's on-site supervision for banks is primarily based on meetings held with the following stakeholders on an annual basis:

- the Board of Directors;
- the Audit Committee;
- the internal auditors;
- the external auditors; and
- one on one meetings with all the risk owners and senior executives.

For insurers, whilst the above is common for the larger insurance groups, a proportionate approach may be adopted for smaller and niche insurance entities.

3

In these meetings the Prudential Authority's analysis of the reports and returns submitted is discussed. Additional information may be requested to give the regulator insight into the organisation and the potential risks which may impact on the supervision of the entity.

The Prudential Authority also uses the "Flavour of the Year" to perform a deep dive into areas of thematic concern for the industry. These are then discussed in the relevant meetings but may require extensive additional reporting.

Off-site supervision

A critical aspect of the Prudential Authority's regulatory requirements is the framework of regulatory reporting which is required by the relevant legislation. The regulatory reporting which is required by the Prudential Authority includes the following:

Banks	Insurers
The suite of BA returns as required by the Regulations to the Banks Act	Quantitative and qualitative reporting as required by the Insurance Act
Internal Capital Adequacy Assessment	Own Risk and Solvency Assessment
Internal Liquidity Adequacy Assessment	Guidance on liquidity risk management of insurers (Insurance Act, 2017: GOI Risk Management for Insurers)
Impact assessments on new legislation	Impact assessments on new legislation
Questionnaires when required	Questionnaires when required
Ad hoc requests	Ad hoc requests

The Prudential Authority (PA) is responsible for anti-money laundering and counter-financing of terrorism supervision of banks, mutual banks, and life insurers. Regulatory developments such as South Africa's demotion to the Financial Action Task Force's grey list will mean more reporting than ever before and its unlikely to stop there. For example, developments in Europe related to sustainability reporting will filter down to South Africa, with increased reporting expected on various sustainability matters (some of which is already in the pipeline).

Other regulators

Amongst others, the following regulators also require reporting from the banking and insurance industries on a regular basis:

- Financial Sector Conduct Authority
- Financial Surveillance Department - South African Reserve Bank
- National Credit Regulator
- Financial Intelligence Centre
- The South African Reserve Bank

Not to mention the reporting requirements, which are not core to financial services, such as SARS reporting, Protection of Personal Information Act (POPIA) reporting, employment equity reporting etc.

3

The impact of these extensive reporting requirements

Following the tsunami of regulation that has been introduced in the last decade, boards and committees are now inundated with internal reporting, paperwork, and analysis. Committee packs are extensive and overwhelming in some instances. The processes to prepare much of this reporting are often manual with significant human intervention.

The challenge for banks and insurers in 2023 is simply how to manage the ever-increasing volume of reporting requirements and regulatory interactions, so that the information derived is meaningful, and not relegated to a checklist. Ensuring internal consistency and meaningful oversight by the board (and the evidencing thereof) requires significant amounts of time and effort.

Possible solutions to the challenge

Banks and insurers have evolved over the years to cater for the extensive requirements of reporting by engaging in the following activities:

- **Automation - the use of RegTech:** RegTech is any technology that uses information technology to improve or supplement a firm's regulatory compliance. Around the world, RegTech investment is ballooning with increasing numbers of firms partnering with RegTech providers to manage the regulatory burden. However, even quick fixes on reports or system requirements can reduce the overall burden.

- **Specialisation:** whilst technology can resolve some of the challenges, having the right people (or advisors) in the right position is more important than ever to ensure regulatory compliance and adequate reporting.

- **Governance restructures:** some firms are insisting on specialist committees that have the appropriate delegated authority to streamline the load within the appropriate control frameworks. These committees require appropriate terms of reference and reporting lines to ensure that nothing slips through, as well as to ensure that relevant and significant issues still find their way to the board.

- **Increased compliance costs and the monitoring thereof:** this is a delicate matter of balancing the need to comply, with constrained budgets, and includes hiring and retaining the right professionals within the organisation (something that is becoming harder to do).

- **Template driven:** setting internal standards for reporting, as well as predefined reporting and measurement threshold, ensures that reporting is easy to understand, consistent, and elevated to the right levels.

For the board, the quality of regulatory reporting is essential to ensuring that all aspects of the business have adequate oversight without distracting from the business of the entity.

Johan Scheepers

Partner
Banking
T: +27 82 492 4463
E: johan.scheepers@kpmg.co.za

Derek Vice

Partner
Insurance
Tel: +27 82 711 2519
E: derek.vice@kpmg.co.za

3

IFRS 17 is live

After much anticipation, *IFRS 17 Insurance Contracts* (IFRS 17) is now live. With an effective date of 1 January 2023, insurers with a December, January or February financial year end are now operating in a live IFRS 17 environment, with insurers with later year ends joining shortly as their new financial years commence. While insurers may have already started producing IFRS 17 reporting in the form of internal management accounts, IAS 8 disclosures in their latest IFRS financial statements (as part of the Standards issued but not yet effective disclosure), and within the QIS submission as required by the Prudential Authority, have largely been limited; with many caveats in place as insurers finalise their IFRS 17 implementation projects.

Reporting in a live environment places additional pressure on insurers to finalise the adoption of IFRS 17 and resolve the caveated / outstanding issues, both on transition as well as business as usual reporting. In the coming months, insurers will need to balance what they report in terms of IFRS 17 results (both internally and externally) – ensuring that this reporting is sufficient to meet requirements and to ensure transparency, with narrative disclosures as required for users to understand the elements that have been finalised and areas of judgement. Too little information may indicate that the insurer is not where they should be in terms of IFRS 17 adoption, but too much information where projects are not yet finalised may result in users of the information placing reliance on results that are subject to change.

Lastly, insurers need to manage the process of ensuring that the IFRS 17 knowledge is transferred from the IFRS 17 implementation project team to those who will be preparing the reporting as part of business as usual – the risk remains that those responsible for reporting may not have been as involved in the IFRS 17 implementation journey and not may fully appreciate the nuances that IFRS 17 brings, resulting in reporting that does not fully encapsulate the IFRS 17 judgements and assumptions.

Lyndall Green

Senior Manager
IFRS 17 Technical Accounting
T: +27 82 710 4976
E: lyndall.green@kpmg.co.za

4 Data and Cybersecurity

4 Data and Cybersecurity

The evolution of cyber risk management

From the boardroom to the boots on the ground: cyber risk management has surpassed the stage of "nice-to-have's" to an essential part of any financial institution's daily operations. The cyber threat landscape continues to evolve and is no longer just a case of keeping organisations resilient as cyber-attack risks grow – but also one of satisfying legislative requirements. This involves an analysis as to what reasonable, technical, and organisational measures to implement to promote cyber operational resilience, whilst ensuring regulatory compliance.

The evolving threat landscape

In an ever-evolving threat landscape the most rational mindset for security teams is to acknowledge that they will never be able to mitigate every type of cybersecurity risk in equal measure. This is a challenging message to communicate to executives, but a necessary one. There must be a balance between protecting against all potential threats versus the onerous cost of security needs.

Given the rapid pace of technological advances and the growing need to protect digital assets, organisations should take the following three (3) key points into consideration:

- In times of uncertainty, trust matters. Digital trust is becoming a boardroom issue. People expect and the law demands that firms act with honesty, integrity and transparency in the way they handle personal information while providing robust, safe and secure digital services. Sensing the public mood, politicians and regulators are acting to shape and challenge corporate behaviours.

- Security teams must change too. It is easy to ignore the need for change in the cybersecurity function itself, but to do so would be naive. Cybersecurity teams are taking on very different roles today. The shared responsibility model brings new partnerships with cloud service providers; shifts to agile Development Security and Operations processes inspires new thinking on embedding security by design; and the security of the enterprise — and customers and business partners — now encompasses a far wider range of systems and assets, often outside the direct control of the Chief Information Security Officer (CISO).

- Be resilient when and where it matters. Despite all the best efforts, the worst can happen. In fact, it's likely inevitable. Resilience is fundamentally a business discussion, not just a security aspiration, and CISOs should resist the urge to assume responsibility for organisational cybersecurity as their sole responsibility. CISOs and their teams can rather function as conveners, encouragers and catalysts for that dialogue across the organisation. CISOs bring a valuable perspective to these discussions as they seek to counter malicious adversaries' intent on disrupting the organisation.

This is representative of the resilience agenda we are seeing in the latest wave of legislation from both international and local regulators, which is of particular importance to financial institutions.

Digital Operational Resiliency Act - Regulation (EU) 2022/2554

The Digital Operational Resilience Act (DORA) is an European Union (EU) regulation that was adopted on 28 November 2022 and which shall apply from 17 January 2025. The growing reliance on digital infrastructure and services, as well as the associated security and resilience threats, are the primary motivating factors behind the development of DORA.[1]

[1] The Digital Operational Resilience Act (DORA) is a Regulation, not a Directive, so it is binding in its entirety and directly applicable in all EU Member States.

4

DORA proposes that a regulatory framework be established for digital infrastructure providers, such as internet service providers (ISPs), operators of data centres, and providers of cloud services, with the intention of ensuring that these providers have the necessary precautions in place to prevent, detect, and respond to cyber incidents.

DORA will apply to the entire financial sector in the EU, including critical third-party providers (CTPPs), such as cloud computing, data analytics or software companies.

Even though DORA is an EU directive, similarly to the General Data Protection Regulation (GDPR), it will become relevant for those organisations that have a footprint and operations in EU countries. In South Africa there are similar legislative obligations that are set out in the Protection of Personal Information Act, 2013 (POPIA), as well as the Cybercrimes Act, 2020 (where it pertains to cybercrime and electronic evidence in criminal cases).

More on the homefront

Whilst companies are still coming to grips with their obligations under POPIA, the Cybercrimes Act will also have an impact on companies doing business in South Africa. The Cybercrimes Act came into partial operation on 1 December 2021. The aim of the Cybercrimes Act is to, amongst other things:

- Create offences which have a bearing on cybercrime, such as unlawful access, unlawful interception of data, unlawful interference with data, computer programs, computer data storage mediums and computer systems, and to criminalise the disclosure of harmful data messages;
- Provide for extra-territorial jurisdiction in respect of cybercrimes;
- Further regulate the powers to investigate cybercrimes and to search, access and seize articles;[2]
- Regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes;
- Provide for the establishment of a designated Point of Contact within the existing structures of the South African Police Service (SAPS);
- Provide for the proof of certain facts by affidavit based on fields of expertise;
- Impose obligations to report cybercrimes on electronic communications service providers and financial institutions;
- Provide for capacity building to prevent, detect and investigate cybercrimes; and
- Provide that the Executive may enter into agreements with foreign states to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes.

It is important to note that the Cybercrimes Act defines a financial institution as it is defined in section 1 of the Financial Sector Regulation Act, 2017 (Act 9 of 2017).

[2] "article" (from Cybercrimes Act) means any—
(a) data;
(b) computer program;
(c) computer data storage medium; or
(d) computer system,
which—
(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
(ii) may afford evidence of the commission or suspected commission; or
(iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission, of—
(aa) an offence in terms of Part I and Part II of Chapter 2;
(bb) any other offence in terms of the law of the Republic; or
(cc) an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic.

4

How does the Cybercrimes Act impact on financial institutions?

- **Reporting obligations**

Section 54 of the Cybercrimes Act places reporting obligations on Financial Institutions, as well as Electronic Communications Service Providers (ECSPs). Section 45, however, is not yet in operation. Once in operation, financial institutions will be compelled to report cybercrimes to the SAPS without undue delay and, where feasible, not later than seventy two (72) hours of becoming aware of the offence and to preserve any *information* which may be of assistance to the SAPS in investigating the said offence.

The challenge at this point is the preservation of such information: preservation implies that the integrity and reliability of the information must be maintained, which could have major cost implications to financial institutions. Although financial institutions might need to put internal processes in place to facilitate this reporting requirement, the provisions of section 54(1) must not be interpreted as to impose obligations on a financial institution to monitor the data which it transmits or stores, or to actively seek facts or circumstances indicating any unlawful activity. This is off course, subject to any other law or obligation that might apply to the financial institution in question. There will only be certainty on what the specific requirements will be once section 54 is in operation.[3]

It is furthermore a criminal offence not to comply with section 54 and financial institutions can upon conviction, face a fine of up to fifty thousand Rand (R50 000).

- **Designated point of contact**

In terms of section 52 of the Cybercrimes Act, the National Commissioner of Police has responsibility to establish a 24/7 Designated Point of Contact (DPoC within the SAPS), which will be responsible for the provision of immediate assistance for the purpose of proceedings or investigations regarding the commission or intended commission of cybercrime offences, or other offences where an "article" comes into play.

- **Assistance during investigations**

In terms of Section 34 a financial institution must provide technical assistance and any other assistance to a police official as may be reasonably necessary in order to search for, access or seize an article. It is a criminal offence not to comply with the provisions of Section 34, and non-compliance may result in a fine or imprisonment for a period not exceeding two (2) years or to both a fine and such imprisonment. Financial institutions should, therefore, ensure that they are in a position to assist the SAPS during investigations, and this assistance may vary from case to case depending on the specific requirements of the investigation and the search.

- **Penalty for non-compliance**

An additional consequence for non-compliance with the various provisions in the Cybercrimes Act, is the potential reputational harm and damage to the Financial Institution, which may have a lasting effect. To mitigate against the risk of non-compliance, financial institutions will need to implement compliance programs to meet their obligations and to revise their compliance frameworks to incorporate any applicable provisions of the Cybercrimes Act into their existing compliance universe.

How does the Cybercrimes Act relate to POPIA?

In certain instances where the personal information of a data subject has been accessed or acquired by any unauthorised person, it could not only be a security compromise that must be reported to the Information Regulator in terms of section 22 of POPIA, but could also be a criminal offence in terms of the Cybercrimes Act.

[3] Section 54 does not apply to a financial sector regulator or a function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989.

In such instances a dual reporting obligation could arise:

- The security compromise must be reported to the Information Regulator as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system (section 22 of POPIA).

- In terms of section 54 of the Cybercrimes Act a financial institution that is aware or becomes aware that its electronic communications service or electronic communications network is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 of the Cybercrimes Act, must without undue delay and, where feasible, not later than seventy two (72) hours after having become aware of the offence, report the offence to the SAPS.

The South African Cybercrimes Act is a major advancement in the fight against cybercrime and in addressing the unique requirements for the search, access and seizure of articles for purposes of criminal investigations. But in all instances the right to a fair trial and the protection of an individual's constitutional rights remain paramount.

Judith Masekwameng

Associate Director
Technology Assurance
T: +27 76 283 6533
E: judith.masekwameng@kpmg.co.za

Advocate Jacqueline Fick

VizStrat Solutions
T: +27 72 133 9188
E: jacky@vizstratsolutions.com

5 Technology and Resilience

5 Technology and Resilience

Technology – are we thinking big (but safe) enough?

The opportunities to use technology to contribute to regulatory compliance, are limited only by our imagination – which equally means creative thinking is needed to ensure technology brings the needed relief / benefits without opening a minefield of unmitigated risk.

Opportunities to use technology to contribute to regulatory compliance

Technology offers a multitude of options – both in well-established and in continually emerging solutions - in solving for (or at the very least, easing the impact of) dynamic and ever-increasing regulatory requirements. Some of the more cutting-edge examples include:

- Using chat-bots to address frequently asked questions around regulatory requirements, compliance related policies, how-to guidelines (e.g., where to find the required documentation or support), and the like.

- Leveraging artificial intelligence (AI) solutions to derive deep insights – e.g., considering multiple data sets holistically (including external information) to highlight trends and / or red flags that may warrant further investigation or reporting in terms of regulations (anti-money laundering, countering the financing of terrorism requirements, ESG reporting etc); or automating more of the financial risk modelling process (including self-learning capabilities within such modelling).

- Utilising established and emerging data and analytics technology (e.g., central repositories – such as data warehousing - to ensure required data for regulatory reporting is hosted in a single location, making the retrieval, verification, and packaging / reporting of such easier and more trusted).

- Applying blockchain technology to store, verify and submit trusted documents - even possibly regulatory submissions (once regulators are able to receive such).

- Using low-code/no-code or process automation technology to automate more mundane or repeatable tasks, such as the generation of defined, standard reporting for regulatory submissions.

What guardrails and broader success factors are needed for technology?

To ensure one addresses internal governance and control requirements (within the agreed risk appetite), plus alleviate regulators' heightened attention, technology-related guardrails will be required. These typically include (to name but a few):

- Technology risk assessment programmes across data, information, technology systems and service providers.

- Continuously monitored internal controls across threat intelligence (detection, mitigation and remediation), identity and access management and vulnerability management.

- Data management and governance (including inventory and classification policies and procedures for structured and unstructured data, recovery and back-up capabilities, access safeguards such as multi-factor authentication etc).

- Data testing, privacy, and obfuscation requirements across the development lifecycle (clearly documented within policies and frameworks, and supported by practical application thereof).

- Frameworks and mechanisms around ensuring trust within Artificial Intelligence (AI) solutions (e.g., to ensure lack of bias, transparency, ongoing verification of self-learning trajectory, etc of the algorithms / underlying calculation engines).

5

- Security incident escalation and responses – ideally automated (including scenario-driven human intervention and feedback loops), to ensure consistent, timely and effective incident communication

- Continuity planning for processes and systems (given due consideration for cyber resiliency, scenario planning and testing, classifications around system criticality etc)

Beyond the purely technical guardrails, a key factor for success in leveraging technology will always be whether it is considered in a more integrated perspective. These broader enablers include for example:

- People: do we have the required skills and capabilities to use and / or support the technology we are bringing on? Are clear roles and responsibilities around all elements of the technology (and broader aspects) established and communicated?

- Change: How will we deal with the change journey in our organisation? Who needs to be brought along in the journey, for inputs in designing the technology – but also for the effective future use thereof?

- Operating model/delivery model: have we got a holistic view of the stakeholders within the regulatory environment, and how we engage or service each of these effectively, especially within heightened automation in our service delivery and ways of working?

- Processes: how are the technology changes impacting our day-to-day processes in regulatory / compliance operations and beyond and how do we bring these up to speed? Can we use the window of opportunity brought by the inevitable change, to drive further process improvements - like automation and streamlining of regulatory reporting?

- Performance insights and data: have we considered how data and reporting needs should be structured to be structured and set-up to address current needs – but to also offer flexibility, sustainability and accessibility for future reporting needs that may come?

- Governance and control: are we sufficiently managing our risks and controls? For example: what is our organisational (board approved) risk appetite and how do we continually monitor and report on this? Can we demonstrate the required frequency and depth of reporting, and ultimately oversight?

While the need to carefully consider the technology related implications and safeguards may seem daunting, it ultimately is worth the "pain" in getting it established, well-running and continuously monitored. Using technology innovatively - balanced with pragmaticism - will play an exponentially increasing role in tackling the burden that regulatory change brings. This becomes especially value-adding in the context of the sheer volume of such requirements; and ultimately in our need to focus our "human" attention on solving the questions of *"So what do we now?", "What does this tell me about the future in the regulatory space and how do I need to adjust now, to give my organisation the best shot at delivering stakeholder value in such a regulated environment?".*

Liesl Slabbert

Partner
Digital Consulting
T: +27 82 718 2872
E: liesl.slabbert@kpmg.co.za

5

Operational resilience – keeping the lights on in times of crisis

Operational resilience is the ability of an organisation to anticipate, prepare for, and successfully adapt to any internal or external disruptions that could threaten the performance of its operations and the services it provides. It requires organisations to actively monitor their operations and take corrective action when necessary to maintain the performance of their operations and services.

A pertinent risk financial services organisations should be considering is the potential collapse of the national power grid in South Africa. Whether it materialises or not, there is benefit in preparing for the outcome as we have seen numerous black swan events materialise in recent years. The country's power supply has already been in a state of crisis, with load shedding and power outages becoming increasingly frequent. A collapse of the national power grid could be catastrophic, causing widespread disruption to businesses and households. Furthermore, the economic impact of such an event would be immense, potentially resulting in job losses, loss of production and data, civil unrest, loss of communications and further strain on the economy.

With escalated stages of load shedding and aging infrastructure, it is anticipated that provincial blackouts and/or extensive power outages leading to a grid failure may follow. Many financial services organisations have performed impact assessments and have developed contingency plans in response to such an incident. Contingency plans should focus on business continuity while considering whether the cost of keeping the lights on outweighs the benefit of the investments involved. The top priority should be safety of people followed by safeguarding critical assets such that recovery of operations is possible following a disruption. Since communication is likely to be impacted, protocols should be in place to ensure key messages are effectively communicated to various stakeholders at the appropriate time using the appropriate available channels. Research has shown that looting becomes rife in such a situation therefore firm plans should be in place with respect to security. Parts of the province have experienced water shedding which may be more widespread in the event of a grid collapse. Supply chains have been put under pressure with the pandemic, civil unrest and flooding in South Africa. Once again, they may be put to the test with diesel shortages, restrictive insurance policies and limited access to critical resources.

When a state of disaster was declared during the pandemic, organisations were steered by regulations and directives from government. Therefore, it is expected that guidelines will follow, especially for essential services and key sectors to avoid the country coming to a standstill. More important than the planning, is awareness and exercising of the strategies to be adopted. While it is perhaps unlikely that a national grid failure may occur, it would be irresponsible not to have it on your risk agenda.

Nashikta Angadh

Partner
Technology Assurance
T: +27 82 719 1368
E: nashikta.angadh@kpmg.co.za

6 Credit and Capital

6 Credit and Capital

Impact of climate risk on expected credit losses

The impact of climate-related risk factors on financial institutions' expected credit loss (ECL) levels will vary depending on the severity and timing of expected climate risks, their direct and indirect impacts on the borrower and on the lender's loan portfolio, as well as the duration of the loan portfolio. The impact on the ECL in the near term is limited, largely because the most significant effects of climate change are only expected to emerge over the medium to longer term. However, it is important to monitor the speed and scale of these matters and consider their possible impacts on the measurement of ECL.

The effects of climate change have been recognised globally as a threat that will impact human, societal, environmental, and economic systems through (for example) rising global temperatures, sea levels and an increasing severity and frequency of natural disasters linked to extreme weather events. It is therefore not a surprise that understanding the impact and reach of climate change is listed as a key priority for many financial institutions. The touchpoints on business may vary from unpacking and reporting the links between climate risk and conventional risks categories (e.g. credit risk, market risk, underwriting risk, operational risk, liquidity risk and reputational risk) to capturing opportunities from the significant client demand for sustainability-linked lending and green loans[1].

The complex interlinkages across the conventional risk types can affect all of the financial institutions' existing financial and non-financial risks. For example, a loan contract might include terms linking the contractual cash flows to a company's achievement of climate-related targets. Those targets affect how the loan is classified and measured (i.e. the lender would need to consider those terms in assessing whether the contractual terms of the financial asset give rise to cash flows that are solely payments of principal and interest on the principal amount outstanding). For the borrower, these targets may affect whether there are embedded derivatives that need to be separated from the host contract.

Incorporating climate-related risks within the ECL measurement

Climate-related matters potentially affect a lender's exposure to credit losses. For example, the consequences of natural disasters (such as wildfires or floods) could negatively affect the borrower's ability to meet its debt obligations to the lender. Further, assets could become inaccessible or uninsurable thereby affecting the value of collateral for lenders[2].

In recognising and measuring expected credit losses, *IFRS 9 Financial Instruments* (IFRS 9) requires the use of all reasonable and supportable information that is available without undue cost or effort at the reporting date. This includes information about borrower-specific attributes, past events, current conditions and forecasts of future economic conditions. Typically, measuring the expected credit losses starts with an estimation of borrower-specific (idiosyncratic) risk, adjusted for the risks posed by the wider macroeconomic environment (systemic risk).

Given this requirement, it is obvious that climate-related matters are relevant in the determination of expected credit losses. The former could for example affect the range of potential future economic scenarios, the lender's assessment of significant increases in credit risk, whether a financial asset is credit impaired and/or the measurement of expected credit losses. In addition, it may impact the expected cash flows to be received from a loan and, therefore, the lender's exposure to credit losses.

[1] Climate related risk drivers and their transmission channels (bis.org)

[2] Effects of climate-related matters on financial statements

6

Borrower-specific attributes risks are generally split into two major categories:

- **Physical risks** - related to physical factors, such as an increase in temperature, as well as all potential consequences from exposure to these factors. An increase in the temperature can for example cause flooding, tsunamis and potentially even impact the frequency and severity of earthquakes.

- **Transition risks** - the risk imposed by transitioning to a greener economy. For example when switching to green energy, the cost of energy initially will go up. Resultantly, properties with high carbon emissions, are considered risky, considering the cost of transition from high carbon emissions to low carbon emissions.

These risks may either individually or in combination, impact expected cash flows as well as the range of potential future economic scenarios considered in measuring the expected credit losses.

Transition risks may impact borrowers who see their business strategies being materially disrupted due to climate change, leading to higher costs of doing business and reduced profitability, increased product obsolescence, the potential for stranded assets and loss of market capitalisation – all of which may impact the probability of default (PD) and loss given default (LGD) of such a borrower.

In addition, we also observe that increased economic uncertainty caused by external events, whether a natural disaster, geopolitical events or pandemics, has had severe impacts across many jurisdictions. Governments, central banks and economists have been revising their economic forecasts to try to incorporate the likely impacts. However, these economic outlooks may change quickly.

The ramifications for expected credit losses described above, will depend on the timing and severity of these changes compared with the period over which the lender is exposed. Therefore, reasonable and supportable information about the extent to which climate-related or economic risks have either already impacted or are expected to impact the borrower over the life of the loan, needs to be considered by the lender in measuring the related ECL.

Lenders may need to consider the impacts of such risks from both a portfolio perspective and a borrower perspective. These risks will impact each portfolio differently, depending on factors such as industry, geography and duration.

Expected credit losses are usually material for financial institutions and other financial institutions and given the challenges posed by the integration of climate-related risk, which will likely require additional resources to updating credit risk policies and ECL models, such as to keep pace with and reflect these changing conditions.

The following factors may be particularly relevant when measuring ECL:

- The increased economic uncertainty about potential future economic scenarios and their impact on credit losses may require financial institutions to explicitly consider additional economic scenarios when measuring expected credit losses.

- ECL models use historical experience to derive links between changes in economic conditions on the one side and customer behaviour, and ECL parameters (e.g. loss and default rates) on the other hand. However, these historical relationships are unlikely to remain stable in times of increased climate and economic uncertainty. Therefore, adjustments to the results from the existing models, based on expert credit judgement and the most recent climate and economic data, may be necessary to reflect appropriately the information available at the reporting date (at least in a first phase, the use of expert judgment based overlays seems more likely than integration of climate risk factors in the statistical credit risk models).

- Certain types of customers, industries or regions may be affected by the increased climate and economic uncertainty more than others. Financial institutions with exposure to these customers, industries or regions will need to consider whether this exposure is captured appropriately in their ECL measurements / parameters.

- Many borrowers may draw down credit lines or hold on to cash to obtain additional liquidity to help them weather the economic storms. This will be relevant for estimating exposures from loan commitments and prepayable or extendable loans.

6

- The expected cash flows used in measuring ECLs may also be affected by any actions planned by the company – e.g., modification, forbearance, limit extensions.

IFRS 9 requires entities to use reasonable and supportable information in measuring ECL. While there is uncertainty over how climate change will unfold and over how clients respond to it, there is ever increasing data about the effects of climate change that would be considered reasonable and supportable information in the context of calculating ECLs. In addition, as reasonable and reliable quantitative data builds up over time (e.g., flood risk data), this will enable the calibration of credit risk models, in such a way as to factor in the correlation of climate-related risk factors to defaults or anticipated defaults and the resulting impact on PD and LGD.

Actions for credit risk management to take now

With the specific regulatory guidance expected to be released by the Prudential Authority (PA) in 2023[3], and the PA's drive to monitor how financial institutions integrate climate-related risk into their governance, risk management and reporting processes, further enhancements to ECL measurements may require the following considerations:

- Consider whether the measurement of ECL appropriately captures the types of customers, industries and/or geographies that are particularly impacted by the economic effects of climate change and which need monitoring for any further acceleration of changes associated with climate-related risk.
- How do the economic scenarios and/or macroeconomic factors have to be adjusted for climate-related risks?
- How should the model results be adjusted, to incorporate / account for expert credit judgement?
- Consider whether risks have been double counted by considering the extent to which the risks might already be captured directly or indirectly through ECL model inputs such as credit spreads, PDs, LGDs and other factors.
- How should credit risk policies and concentrations of credit risk be highlighted for sectors that are more exposed to climate-related risks?
- Consider how clear and meaningful disclosures have been provided about significant judgements, assumptions and estimates made.

Due to the significant challenges that climate-related risks pose to financial institutions in relation to their traditional approach of identifying and quantifying these risks, and given the unique characteristics of climate-related risks (including the extensive breadth and magnitude of these risk over prolonged time horizons); it is fundamental for financial institutions to assess the relevance of climate risk drivers and how these can be incorporated into ECL measurements. Ultimately, it boils down to keeping up with available information around climate risks and their impacts; and continuously checking and evolving the related financial modelling. This will have broader reaching consequences to financial institutions (i.e., beyond purely adjusting models for changing circumstance) – such as bolstering of expertise and capacity to deal with the required monitoring and modelling.

Maria van der Valk

Partner
Financial Risk Management
T: +27 82 712 7878
E: maria.vandervalk@kpmg.co.za

Alec Slabbert

Associate Director
Financial Risk Management
T: +27 79 617 5919
E: alec.slabbert@kpmg.co.za

[3] Prudential Communication 10 of 2022 - Climate-related Risks.pdf

7 Scrutiny and Divergence

7 Scrutiny and Divergence

Cartel conduct, the simplest of enquiries – or perhaps not?

Cartel conduct – the line is blurred

Surely it is a simple enquiry. You either participated in cartel conduct or you didn't. What could be difficult about confirming whether two competing companies fixed a purchase or selling price, fixed a trading condition, allocated customers, suppliers, territories or goods or services between them or engaged in collusive tendering? After all, cartel conduct in terms of section 4(1)(b) of the South African Competition Act ("**the Competition Act**") is legally regarded as anti-competitive per se and no technological, efficiency or other pro-competitive justifications can be raised as a defence. Furthermore, the Competition Commission does not have to prove an anti-competitive outcome. Such an outcome is presumed given the serious nature of cartel conduct.

But history has told us that things are often not as easy as they seem. It is sometimes hard to distinguish between legitimate commercial behaviour and collusive conduct which contravenes the Competition Act. The characterisation of horizontal agreements between competitors was a hot topic of discussion between the panellists at the 2022 Annual Competition Conference of the Competition Commission ("The Commision"). The panellists reflected on the successes achieved by the Commission in busting hard core cartels but also on some of the headwinds experienced by the Commission and some of the cartel cases it has lost. The importance of properly characterising alleged cartel conduct to confirm whether it squarely falls within the ambit of section 4(1)(b), was emphasised.

The observation was also made during the panel discussion that the line between cartel conduct contemplated in section 4(1)(b) and general anti-competitive behaviour between competitors in terms of section 4(1)(a) needs to be further clarified. This is an important distinction as a complaint based on section 4(1)(a) will require the Commission to show a substantial prevention or lessening of competition in the market while the respondents will be able to bring evidence of technological, efficiency or other pro-competitive gains to justify their conduct. This distinction is further important as the legislature only introduced criminal liability for cartel conduct in terms of section 4(1)(b) and not for general anti-competitive conduct between competitors in terms of section 4(1)(a).

Information sharing guidelines

The Competition Commission is well aware of the difficulties experienced by market players to distinguish between lawful information sharing and anti-competitive or collusive information sharing. The need for clarity is particularly prevalent among members of trade or industry associations. In 2017, the Commission published draft Guidelines on the Exchange of Information between Competitors under the Competition Act ("2017 Draft Guidelines") for public comment. The Commission intentionally made these guidelines broad in an attempt to deal with as many forms of information exchange among competing market players as possible. However, after receiving extensive comments from interested parties, the Commission published amended and more focussed draft guidelines in 2022 called "Guidelines on the Exchange of Competitively Sensitive Information between Competitors under the Competition Act" ("2022 Draft Guidelines"). Following a period for public comment, final guidelines ("2023 Final Guidelines") were published on 24 February 2023.

While the 2017 Draft Guidelines referred to "commercially sensitive information", the 2022 Draft Guidelines and the 2023 Final Guidelines refer to "competitively sensitive information" and place the emphasis on and warn against the sharing of information which is important to the rivalry between competing firms.

7

They describe the potential harm associated with information sharing with reference to factors such as the level of concentration and product differentiation in a market, the age of the information and the level of detail being shared between competitors.

In this regard, the sharing of information between competitors in a concentrated market with a low level of product differentiation is likely to attract the attention of the Competition Commission, especially if the information being shared is current or future looking and in such a disaggregated form that the competitively sensitive information of an individual competitor is visible to other competitors in the same market. The Commission's main concern is that such information sharing could potentially facilitate a collusive understanding between competitors or support the monitoring of compliance with a collusive agreement, in other words a cartel.

Complex topics not dealt with

The 2022 Draft Guidelines and the 2023 Final Guidelines are much shorter and more focussed than the 2017 Draft Guidelines. The Commission mentioned in the Explanatory Note to the 2022 Draft Guidelines, that it chose to omit certain complex topics from these guidelines as it felt that these topics need to be considered on a case by case basis. A quick read of these topics tells us that they are not only complex in nature but also highly risky from an information sharing perspective. The omitted topics are price signalling or public announcements, joint ventures, cross-directorships, cross-shareholding, customer requests for quotations and market studies and benchmarking.

The sanctions cannot be ignored

There is no margin for error, as a contravention of the Competition Act could result in administrative penalties as high as 10% of turnover or 25% of turnover for repeat contraventions. There is also criminal liability to worry about when dealing with cartel conduct. Always give early consideration to potential platforms for information sharing between competitors so that potential risks can be avoided or mitigated. Trade or industry associations, in particular, need to be extra careful and members of such associations need to ensure that their representatives not only understand the risks associated with information sharing between competitors but also receive clear guidance on measures to be applied to prevent any collusive or anti-competitive outcome.

Anton de Bruyn

Director
KPMG Law
(a business unit of KPMG Services (Pty) Ltd)
T: +27 82 719 0317
E: anton.debruyn@kpmg.co.za

7

Transfer pricing under the microscope

Transfer pricing has been a buzz word for a few years, ***but what is transfer pricing?*** Transfer pricing refers to the prices of goods and services that are exchanged between companies under common control. For example, if a subsidiary company sells goods or renders services to its holding company or a sister company, the price charged is referred to as the transfer price. Transfer prices between related parties are required to be at arm's length.

Why is transfer pricing a focus area and why are regulators paying so much attention to transfer pricing?

Multinational Corporations ("MNCs") are legally allowed to use the transfer pricing methods for allocating earnings among their various subsidiary and affiliate companies that are part of the same group. However, companies at times can also use (or misuse) this practice by altering their taxable income, thus reducing their overall taxes.
The transfer pricing mechanism is a way that companies can shift profits. Profit shifting is when MNCs reduce their tax burden by moving the location of their profits from high-tax countries to low-tax jurisdictions and tax havens. Hence, transfer pricing is high up on the radar for regulators and tax authorities to ensure that Balance of Payments and Tax Bases in their respective jurisdictions are not being eroded.

Based on data available, the matter of Base Erosion and Profit Shifting ("BEPS") was perceived to be so significant that the Organisation for Economic Co-operation and Development ("OECD") embarked on a project to build an Inclusive Framework on BEPS to bring together a number of countries around the globe to collaborate on the implementation of the OECD/ G20 BEPS Package. The first actions were rolled out in October 2015 (popularly known as BEPS 1.0) and the evolution of the BEPS continues till date with new proposals (also know as Pillars) under the BEPS 2.0 program.

[Base erosion and profit shifting - OECD BEPS]

As technology and consequently businesses evolved, the political boundaries became blurred. To encourage investments and support government strategies of ease of doing business, central banks and regulators were required to liberalise their strict exchange controls. Set policies or limits faded away and in some instances safe harbours have been introduced. Business models have become more complex and MNCs can approach the central banks and relevant regulators for approvals on transaction pricing that could go way beyond the safe harbour limits (e.g. interest rates on loans or payment for intellectual property). However, robust economic support and viability for such requests needs to be provided and transfer pricing is the basis on which such support can be presented.

On the one hand, based on relevant support provided, the central banks and regulators have started allowing aggressive pricing of intra-group transactions, but on the other hand these practices could lead to BEPS and hence the revenue authorities have stepped in to protect and enhance the tax base in their jurisdiction. A number of legislative amendments and enhancements have been made in this regard.

Included below are typical types of transactions that require exchange control approval or notification:

- **Intellectual property (royalty, franchise fees and technical fees):** MNCs use Intellectual property (IP) structuring models to separate the ownership, funding, maintenance and use rights of intangible assets from the actual activities and physical location of intangible assets. This allows them to operate in a manner that the income made from the intangibles in one location is received in another location with a low no tax regime. For example, MNCs can establish IP holding companies in suitable offshore locations to acquire, exploit, license or sublicense IP rights for their foreign subsidiaries. Profits can then be shifted from the foreign subsidiary to the offshore IP holding company where low to no taxes are applied on the royalties earned.

7

In addition, many countries allow for enhanced deductions or provide incentives with regard to expenditure on Research and Development ("R&D"). MNCs can set up R&D facilities in countries where the best tax advantage can be obtained making use of an attractive R&D infrastructure and tax incentives and benefit in another country with low/no tax on the income derived from exploiting such R&D.

These structures are common in the financial services field where IP plays a large part in the digital presence and success of the organisation. While these structures are not illegal, regulators and revenue authorities keep a close watch on these structures and it is important to demonstrate to them that these structures have not been set up for BEPS.

- **Management or administration fees:** Similar to IP fees, management and administration fees are closely monitored transactions and are quite common transactions in financial services organisations. Demonstrating value or benefit of the services for the service recipient is key.

- **Interest:** The mobility and fungibility of money makes it possible for MNCs to achieve favourable tax results by adjusting the amount of debt in a group entity and hence interest deductions. While certain regulatory safe harbours exist for interest rates, given the recent economic cycles, debt commands a much higher interest rate that the set safe harbours determined originally. Hence, with appropriate justification, central banks have in recent times been known to have approved debt carrying extremely high interest rates.

- **Transfer pricing adjustments (true up/down):** This is a mechanism whereby the price of goods or services is adjusted to provide a pre-determined return to an entity in the value chain. The invoices/credit note/debit note for these adjustments are typically not accompanied by a delivery of goods or services (as these are adjustments for historical transactions) and hence regulatory approvals become important to enable the flow of money to give effect to these adjustments. These transactions are not very common in the core financial services transactions, but exist in the peripheral activities such as management fees, R&D, etc.

It is important to note that prior to any agreement with regard to the above-mentioned transactions becoming effective, the approval of the Financial Surveillance Department of the South African Reserve Bank or, where it is permissible, the prior approval of the Authorised Dealer must be obtained.

Getting the balance right

Good transfer pricing analyses and documentation are key to balance transaction models and values for central banks, regulators and revenue authorities to rely on and accept, to avoid difficulties in regulatory approvals and also avoid unnecessary tax costs where transfer prices do not satisfy the arm's length test.

It is recommended that appropriate transfer pricing policies and documentation be maintained for existing transactions that could require a continuous renewal of regulatory approvals. Business models are constantly evolving and hence newer transactions may be implemented as a result of such evolution (e.g. outsourcing activities or IP structures). It is important that a robust transfer pricing analysis be undertaken to build the commercial rationale for such transactions to be presented to regulators to obtain approvals.

Amit Chadha

Partner
Global Transfer Pricing Services
T: +27 79 130 8540
E: amit.chadha@kpmg.co.za

8 Fraud and Financial Crime

8 Fraud and Financial Crime

Disregarding privacy to combat fraud and financial crime

The question that arises is: how is privacy protected when private companies are being made public?

In response to the Mutual Evaluation Report of South Africa published by the Financial Action Task Force ("FATF"), the promulgation of the General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act 22 of 2022 ("General Laws Amendment Act") will effect the first substantial amendments to the Companies Act 71 of 2008 ("Companies Act") since its enactment in 2011. However, the increased company compliance obligations may be burdensome and will weigh heavily on the right to privacy of individuals who are ultimately in control of South African companies.

Remediating the findings of FATF

The Mutual Evaluation Report of South Africa published by the FATF analysed the level of effectiveness of South Africa's 'Anti-Money Laundering and Combating the Financing of Terrorism' ("AML/CTF") system and provided recommendations on how the system could be strengthened. South Africa was afforded the opportunity to remediate the deficiencies identified by the FATF and implement the 40 FATF recommendations to avoid being grey-listed, a move we now know was not sufficient to prevent South Africa from being placed on the FATF grey list. Motivated by principles of transparency and accountability, the General Laws Amendment Act seeks to addresses fifteen of the twenty deficiencies identified by FATF by amending five separate South African Acts.

The effects of the amendments to the Companies Act

From 1 April 2023, the General Laws Amendment Act will require:

- Every company to submit a copy of its securities register simultaneously when filing its annual return at the Companies and Intellectual Property Commission ("CIPC");
- If a company is a regulated company, or if it is controlled by or if it is a subsidiary of a regulated company, in terms of the Companies Act, such companies will be required to include a register of the disclosure of beneficial interest when filing its annual return at the CIPC; and
- All other companies will be required to regularly file a record with the CIPC with information regarding individuals who are the beneficial owners of a company.

A beneficial owner is defined as an individual who, directly or indirectly, ultimately owns that company or exercises effective control of that company. This includes instances where an individual can materially influence the management of the company.

Companies will also be burdened with having to identify the chain of holders of beneficial interest to determine who is the ultimate owner of its securities, whether they exercise control over the company or not. They will need to file and regularly update the record of such beneficial ownership at the CIPC.

The impact of the FATF recommendations in the European Union

In accordance with the FATF recommendations, by 2015 most jurisdictions in the European Union ("EU") with an AML/CTF regime implemented central beneficial ownership registers which contained accurate and up-to-date information on the beneficial ownership of legal persons or legal arrangements, accessible by persons or organisations that could demonstrate a "legitimate interest" to access those records.

8

It provided more legal certainty in relation to transactions or business activities with such legal persons or legal arrangements, reducing the risk of fraud and other financial crimes. The beneficial ownership registers included personal information such as the ultimate beneficial owner's name, month and year of birth, country of residence and nationality.

In 2018, the EU extended the access to beneficial ownership registers to any person of the public. Personal information was further made public when the EU's beneficial ownership registers interconnection system was created, linking all EU member states national central registers containing beneficial ownership information. However, unfettered access to beneficial ownership registers may be seen as an unjustifiable violation of an individual's rights to privacy. In this regard, it was decided by the Court of Justice of the European Union in 2022 that, while it recognises that giving the public access to beneficial ownership information increases transparency and contributes to the prevention of money laundering and terrorist financing, general public access is unnecessary and disproportionate, and such access cannot justify its interference with privacy and the protection of personal information, therefore countries should consider limiting such access to persons and organisations with "legitimate interest".

A consideration of the right to privacy in the context of a South African company

The Companies Act of South Africa encourages transparency and high standards of corporate governance given the significant role of companies within the social and economic life of South Africa. The Promotion of Access to Information Act 2 of 2000 ("PAIA") particularly promotes transparency, accountability and effective governance of all public and private bodies and justifiably limits the right to privacy. This becomes a balancing act. Although there is the constitutional right to privacy which is now enshrined in the Protection of Personal Information Act 4 of 2013 ("POPIA"), this right is not absolute and is subject to justifiable limitations aimed at protecting other rights and important interests.

The privacy risks the amendments will create

The amendments are not clear regarding the accessibility of companies' securities register to the public. In this regard, the amendments state that the CIPC must make the annual return electronically available to any person as prescribed. This means that unless limitations to accessing annual returns are developed, any person will have access to a company's annual financial statements as well as the details of the shareholders and beneficial owners (such as their name, address, and shareholding interest). Not only does the publication of such personal information render the distinction between a private and a public company uncomfortably superfluous, but public accessibility (if not appropriately limited) poses a risk of wealthy individuals being targeted by persons for nefarious purposes.

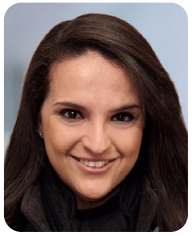
Who should have access?

It will be important for the Minister of Finance, after consultation with the Financial Intelligence Centre, to carefully consider which persons should have access to annual returns taking into account the data privacy rights of shareholders and beneficial owners in terms of POPIA. This determination should be considered in light of reasons driving the amendments to the Companies Act. If we presume that these reasons are to strengthen South Africa's anti-money laundering systems and combat the financing of terrorism, there is a strong case that such personal information should only be made available to law enforcement officials who have a reasonable and, perhaps, lawful purpose for requiring this information, as is the case in the EU.

8

Adapting to the change

Proposed changes to the Companies Act have been looming since 2018, with the revised Companies Amendment Bill being published as recently as 1 October 2021. Enacting the amendments highlighted above ensures greater transparency to mitigate against companies being used as vehicles for criminal activities in South Africa. Although unmasking the individuals who ultimately own or exercise effective control of the company will be a welcomed deterrent for fraud, corruption and financial crimes that cripple South Africa's economy, it should not come at too high a price by making sensitive personal information of individuals publicly available. In our view, it is important for the Minister of Finance to prescribe limitations to the accessibility of annual returns thereby balancing the right to data privacy against the right to access information in the public interest.



Nada Ford

Manager
Legal Services
(a business unit of KPMG Services (Pty) Ltd).
T: +27 72 686 1161
E: nada.ford@kpmg.co.za

8

South Africa has finally been grey-listed by FATF, what is next?

On 24th February 2023 the Financial Action Task Force (FATF) published its decision to include South Africa on the FATF list of "jurisdictions under increased monitoring", also commonly known as the FATF "Grey List". This result, though disappointing, was already long anticipated as it is simply not possible. to remediate the 20 negative ratings out of the 40 FATF technical compliance standards that our anti-money laundering and counter-financing of terrorism (AML/CFT) regime obtained in one year.

Removing South Africa from the Grey List should be now a national priority, as the longer we stay on the Grey List, the more aggravated the negative impact could be. In this sense, the South African government has already asked the FATF to reassess South Africa during its Plenary in June 2023, in which hopefully our recent legal and regulatory changes may contribute to the re-rating of some of our negative compliance results. However, we are still very far from being removed. As an example Mauritius was only removed from the Grey List in October 2021, even though two follow-up assessment took place in 2019 leading to different positive re-ratings.

While the regulatory environment is expected to become increasingly strict and with rapid changes, financial institutions need to be more proactive undertaking transformation process to implement the necessary progresses in their AML/CFT controls, including the following:

- Automation and digitalization of Know Your Customer (KYC), ongoing monitoring and suspicious activities detection processes;
- Provision of sufficient authority and capacity to compliance functions to construct robust assurance framework to supervise the 1st line of defense;
- Ensure the identification and understanding of customers and of their beneficial ownership; and
- Materialize all the controls described in the Risk Management and Compliance Programmer in duly implemented processes;

We can only achieve removal from the Grey List if all stakeholders in the public and private sector work together to fulfil the Action Plan as established in the FATF Plenary Outcom in the next three years. While many initiatives need to be taken by public sector authorities, private entities still have a long way to go to implement truly effective AML/CFT mechanisms instead of a tick-the-box rule-based compliance exercise.

Monica Wu

Senior Manager
Forensic
T: +27 72 446 7281
E: monica.wuyu@kpmg.co.za

9 Fairness and Inclusion

9 Fairness and Inclusion

The purpose and pitfalls of complaints management

The unbearable cost of human progress

Democracy, the human rights movement, and liberalism have been a boon to humanity – increasing life expectancy, ameliorating quality of life, and uplifting people and communities. These precious benefits do not absolve it, however, of its most prominent crime… the "Rise of Karen". Karen is a corrosive phenomenon that threatens to eclipse all human progress, and to destabilise civilizations.

Who is Karen? Karen is the complainer who exaggerates not only the injustices she is forced to endure, but also her entitlements, her privileged access to the true version of events, her superiority over the everyman (specifically shop assistants, call centre agents, waiters, and the elusive "your manager"), and her ability to swiftly bring balance back to the consumer force.

The nature of complaint

The offences of Karen's across the globe do not mean we should dismiss complaints out of hand. Instead, the contemporary accusation that someone is a "Karen", or the timely warning not to "go all Karen", hints at the ambiguity at the heart of "complaint". Like with exercise and red wine, complaining also requires moderation… and judgement. If we never complain we might be suffering from "pushover-ism" – a deficiency of self-regard, and a lack of proper moral outrage at injustice. On the other hand, if we complain too much, we could be diagnosed with chronic Karen-ism – delusions of grandeur, and misplaced outrage.

The truth is, the very possibility of Karen demonstrates moral progress in the course of history. Complaints assume a measure of recognition. As a rule, slaves didn't get to lodge complaints. And kings generally didn't suffer criticism of their rule from their subjects. When a contract is negotiated between equals, however, or when one or both parties in a relationship are afforded certain rights, then dissatisfactions can be aired. It means that the interests and legitimacy of each party is recognised. While some of us get complaints wrong some of the time, we should be happy that complaining is possible.

The role of complaints in financial services

Financial services, like many other industries, have in the past mistaken the person for a policy. In the process we've harmed people who could have been our mothers, our brothers, our children. In 2018, for instance, the Banking Royal Commission in Australia found, among other things: call centre agents sometimes cold-selling policies to mentally challenged individuals; insurance premiums charged to deceased people; delays in urgent home repairs for disaster victims; and misleading car and travel cover.

The problem is that the individual policyholder with a legitimate complaint may still experience challenges when seeking answers and fairness from giant, anonymous and bureaucracy-driven institutions that provide financial services. There is comfort in being insured by a big institution. Managing thousands of policies consistently and fairly requires a necessary component of bureaucracy. Unfortunately, such systems may also hamper service and hinder fairness.

9

Complaint procedures are therefore not merely mechanisms for managing reputational risk, or for keeping regulators at bay. Complaint procedures are attempts to ensure fairness for the customers to whom we've promised protection and peace of mind. Through complaints we can track the organisational virtue of justice.

The dangers of compliance

Apparently business historians track the first recorded consumer complaint to ancient Mesopotamia. The first Karen was clearly wealthy, given that she could immortalise into a clay tablet her dissatisfaction with the quality of copper she received… in 1750 BC. The same historians claim that complaints haven't really changed much – we still complain about the quality of goods, unexpected costs, and the breakdown of trust when promises are broken.

Frequent complaints in insurance relate to claims handling, including unsatisfactory settlement offers, claim delays, and denial of claims. Other often encountered complaints pertain to policy costs and cancellation.

It can be frustrating and difficult for policyholders to have complaints resolved, and because financial institutions have been guilty in the past of unfair treatment, regulations today outline detailed requirements related to complaints procedures. This includes (among a host of other requirements)[1]:

- documented procedures for managing and categorising complaints;
- appropriate complaint record keeping, monitoring and analysis of complaints, and reporting (regular and ad hoc) to executive management, the board of directors and any relevant committee of the board; and
- a process for managing complaints relating to the insurer's service providers.

While the regulations seem like a sincere attempt to ensure that complaints are taken seriously, there is also the devilish and ironic possibility that we are trying to solve a lack of humanity in the industry with more bureaucracy. One cannot help but be reminded of Graeber's law here[2]:

…any market reform, any government initiative intended to reduce red tape and promote market forces will have the ultimate effect of increasing the total number of regulations, the total amount of paperwork and the total number of bureaucrats the government employs.

Graeber has government bureaucracy in mind, but the logic applies equally to corporate governance. In an attempt to increase care, we default to data, digitalisation, tracking and reporting – what Graeber has elsewhere referred to as the BS-ification of work.

The warning here is therefore to keep the person behind the policy in view while we track complaints on spreadsheets. The challenge for financial institutions is to find ways to return to the essence of compliant (i.e., "recognising people"), and to avoid (a) creating additional barriers to fairness, and (b) allowing the mountains of data we collect about policyholders to obscure our view of them.

Heightened scrutiny from our regulators in this regard is inevitable. Complaints data (or the lack thereof) gives regulators an inside view of business practices and the culture of the organisation. The UK's new Consumer Duty is an indicator of just how rigorous regulators are prepared to be to ensure the necessary standard of care and fair outcomes for customers. The Financial Conduct Authority (FCA) has clearly communicated to firms that they need to "consider the needs, characteristics and objectives of their customers – including those with characteristics of vulnerability – and how they behave, at every stage of the customer journey." They take this even further, requiring that firms not only act to deliver good customer outcomes, but also evidence whether those outcomes are being met. Quality complaints data is going to be a big part of meeting this requirement.

[1] Cf. Policyholder Protection Rules (Long Term Insurance), 2017, Rule 18 (Section 62, Long-term Insurance Act 1998).

[2] Anthropologist David Graeber, author of Bullshit Jobs, Debt: The First 5000 Years, and The Dawn of Everything proposed the "Iron Law of Liberalism" in The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy (2015).

9

Mindful complaints etiquette

A recent study found that Karen-like behaviour will most likely be displayed, not by people named Karen, but by Louise's, Ann's and Jane's. The study also tried to pinpoint where across the globe one is most likely to encounter a Karen, and to provide tips for businesses in dealing with Karen's. These tips include:

- Keeping calm;
- Staying solution-focused; and
- Sticking to the facts.

Being prepared for irrational complaint seems prudent. But it should be borne in mind that irrational complaint is the exception. The majority of complaints involve at least a measure of legitimacy and rationality. If a financial institution has the genuine aim to enhance the lives of people – as most of them claim – it would behove them to create products and manage claims in a manner that makes complaint and complaint procedures unnecessary. We live in an imperfect world and because we are imperfect people (as policy providers and policyholders) the next best thing is to recognise complainants and to address complaints with a view towards fairness.

Schalk Engelbrecht

Chief Ethics Officer
Risk Management
T: +27 82 713 7656
E: schalk.engelbrecht@kpmg.co.za

Michelle Dubois

Senior Manager
Regulatory Centre of Excellence Lead
T: +27 60 997 4512
E: michelle.dubois@kpmg.co.za

[3] Available at: The Karen Capitals: Who & Where Complains the Most? | Bionic

10 Risk and Governance

10 Risk and Governance

Interconnectivity of risks

Moving into 2023, the world faces risks that feel both wholly new and eerily familiar. We have seen a return of "older" risks – inflation, cost-of-living crises, trade wars, capital outflows from emerging markets, widespread social unrest, geopolitical confrontation and the spectre of nuclear warfare – which few of this generation's business leaders and public policy-makers have experienced before.

These are being amplified by comparatively new developments in the global risk landscape, including unsustainable levels of debt, a new era of low growth, low global investment and de-globalization, a decline in human development after decades of progress, rapid and unconstrained development of dual-use (civilian and military) technologies, and the growing pressure of climate change impacts and ambitions in an ever-shrinking window for transition. Together, these converge to shape a unique, uncertain and turbulent decade.

The need for businesses to monitor rapidly shifting public opinion is nothing new. However, in 2022, heavily polarized political and cultural pressures weaponized through social media, means no company is sheltered. Risks include consumer boycotts, reputational damage and legislative crackdowns from regulators who either perceive certain businesses as acting against the national interest or feel the political need to please voters, disgruntled with what they see as business' failure to champion causes they hold dear.

Businesses cannot plan for every potential exogenous threat. Still, if they misjudge what they should prepare for, companies which are effectively adept at understanding these less easily definable exogenous threats will be better prepared to manage risks and their consequences.

We may be induced into a false sense of security because, in a globally interdependent world, the traditional (and predictable) risks of the past are evolving into highly complex uncertainties that we cannot map, predict, and anticipate. Business leaders often fail to distinguish between risks and uncertainty. The critical difference is that the outcomes (and possibly even the likelihood) of 'risks' are more ascertainable and fathomable to the human mind. Whereas 'uncertainty' is, by definition, characterized by a lack of information.

These complex and yet discrete actions are more difficult to identify. However, a range of base-case alternatives and worst-case scenarios around regulatory shocks, protectionism and 'weaponized' trade and economic policy can and should nevertheless be articulated and assessed. In this sense, the principal value of the exercise lies in the process of:

- Imaging and stress-testing as many possible scenarios that can affect, positively or negatively, your business;
- Differentiating between more predictable and definable risks from more complex, seemingly unfathomable, impacts (uncertainties); and
- Finally determining strategies that minimize negative effects and maximize favourable outcomes.

The aim of the process is to become comfortable in dealing with uncertainty and preparing your organisation for it, ultimately resisting and even improving from the impact of random events.

This is precisely what interconnected risk assessment attempts to do, as a starting point, by uncovering hidden insights and cutting through the complexity around the potential 'connection' and 'impact' effects of risks.

Developing risk management processes to anticipate and mitigate the predictable outcomes of more definable threats have long been in use. However, developing strategies to deal with more complex, undefinable events is the next step in corporate mitigation strategy.

10

We need to consider whether and how risks can potentially cluster together and the potential cumulative impact of such clusters. We must advance beyond historical risk analyses comprised of two-dimensional depictions through expected probability and severity.

In a world where economic volatility is the norm and the past is no longer an indicator of things to come, disparate events can become inextricably linked. This makes assessing risk exposure especially difficult because risk is unpredictable and contagious and connected globally within complex organizational structures. We may have reached a tipping point where traditional, two-dimensional risk management methodologies that focus on single points of risk with high likelihood and severity may provide only limited value and insights in increasingly complex and globally interconnected organisations.

Combining the latest in applied science with insights from management, and extensive benchmarking, interconnected risk assessment modelling allows us to observe where risks can be expected to form critical clusters or trigger 'contagion' with other risks. We can objectively measure the genuinely significant threats by exposing the expected contagion effects between global and enterprise risks.

This approach combines qualitative and quantitative data to help identify the following:

- Your greatest systemic risk exposures, combinations, and risk clusters to inform a risk mitigation plan;
- How risks will impact each other in the network and how they behave in a dynamic manner over time;
- The impact of "mega trends" and their effects on your business;
- Insights that may help you improve mitigation of systemically critical risks to aid you in developing an investment strategy to counter those weaknesses; and
- A framework to revisit the risk tolerance statement and overall risk management strategy.

This process and approach can be summarised as follow:

Risk identification - work with key stakeholders to identify the key internal and external risks facing the organisation. These risks can be technological, financial, social, or cultural, amongst others, and can be unprecedented and/or behavioural, i.e., quantitative data on them is limited.

Survey - key stakeholders complete an online survey for the collection of data on the characteristics of the risks facing the organisation.

Analysis - apply advanced network theory to the aggregated survey responses to identify the organisation's interconnected risk network and its dynamics. Network theory enables the user to quantify the risks, leading to actionable outcomes.

Report – these modelling results reveal where risks can be expected to form critical clusters or trigger 'contagion' with other risks. Focusing on systemic risks helps produce agile risk management and enhances strategic decision-making.

Adopting an interconnected risk assessment approach, analyzing the results and implementing the associated strategy and action plans will assist organisations in better understanding the interconnectivity of risks and the manner in which they need to respond to these challenges.

Rainhard Muller

Associate Director
Internal Audit, Risk & Compliance Services
T: +27 82 719 6384
E: rainhard.muller@kpmg.co.za