KPMG

Ten key regulatory challenges of 2025

Pressure is the future we shape

kpmg.co.za

Introduction

On behalf of KPMG's Africa Regulatory Centre of Excellence, I am delighted to share our flagship publication – The Ten Key Regulatory Challenges of 2025.

In this year's publication we focus on how the intensity of regulatory pressure shapes the future of financial services firms. Successful firms will leverage the increasing scrutiny to unlock efficiency and growth potential. It's a delicate balance between allocating resources and increasing spend on seemingly non income generating activities while at the same time investing and building a business that can embrace the pressure from regulators.

We have identified what we believe are the ten key regulatory challenges for the year ahead and look forward to engaging with you to discuss how you are shaping the future of your firm, amid increasing regulatory pressure.

- **Geopolitics**
- **Financial Crime**
- **Cyber**
- **Data Privacy**
- **IT Governance**
- **Tax Transformation**
- **Payments**
- **Operational Resilience**
- **Climate and Sustainability**
- **AI Governance**

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 2025

Geopolitics

Geopolitics

Playing the Trump card

Economic fundamentals in the US and Europe may have signalled that 2025 will be a year of some normalisation and consolidation, as far as normalisation is fathomable amidst the ongoing conflicts. Global inflation driven by post-pandemic public spending and supply chain disruptions is slowing and created the space for central banks to reduce interest rates, all of it favourable for supporting investment and growth. It will, however, most likely not be such a year.

Eliciting reactions across the political spectrum

As the world readies itself for the global effects of the second Trump administration, it is clear that President Trump intends to be consequential. Headlines following his first day in office, reporting on the multitude of newly signed executive orders, use descriptors like "massive" and "sweeping" to predict the disruption that may follow his policy directives. These include his approach to trade and tariffs, foreigners, diversion, equity and inclusion, the LGBTQ+ community and other minorities, World Health Organisation membership, participating in the Paris Climate Accord, control of the Panama Canal, and ownership of Greenland, to mention a few.

There is much global uncertainty about the implications of his proclivity for "sweeping", disruptive action to achieve objectives he deems in America's national interest, irrespective of broader or even longer-term repercussions. Although President Trump did not attend the 2025 meeting of the World Economic Forum in Davos, the potential implications of his presidency dominated almost every discussion. His inward focus, an adversarial us-versus-them view of the world, may have favourable spin-offs in a hereto relatively rules-based world order that traditionally looked towards the US to offer not just resources but also ideological leadership. This role, which was also used to export and proliferate a value system, has spurred US involvement in global conflicts such as those in the Ukraine and Gaza. President Trump's unwillingness to use American resources in ways that do not directly benefit American citizens may add pressure towards early termination of these conflicts, although possibly with less desirable end results. It may however also fuel the decline of rules-based international diplomacy and further polarise alliances delineated by powerful individuals rather than value systems to produce intimidation theatre on a world stage where strong men assume position against each other. As the saying goes, when elephants face off, the greatest risk is to the grass.

The world is watching

The net effect of the apparent contradictions in his pronouncements about the future policy directions he plans to take is difficult to compute. For one, he promises to improve the lives of Americans through jobs, economic growth and lower prices. In his accounting, large-scale deportation of foreigners factors positively into this equation. Apart from the human cost, the fiscal implications of such an endeavour will burden American taxpayers enormously, vacate many crucial, low-paid jobs and drag economic growth down. Threats of tariffs on imports from especially China will similarly price imported inputs higher. This will slow growth and fuel price increases — conspicuously not the utopian turnaround or " Golden Age" promised in his inauguration speech. Having witnessed his proclivity for dramatic action however, the world takes him seriously and is jittery. In anticipation of potentially disruptive trade wars, some trading partners have adapted trade policies with the US even before the inauguration, rendering his threats very effective. Such is their credibility, that he has no need to actually implement the retaliatory trade policy he promises to visit on trading partners who do not adhere to his norm of "America first". They simply fall in line.

Tax cuts are a favourite in President Trump's proposed growth stimulus. This may in fact benefit the wealthy and again put the already disproven trickle-down economic theory to the test; it may simply exacerbate inequalities further and not help the disposable income of low-income earners much. Tax cuts are feasible only when public expenditure is curbed too, raising questions about changes in state-provided social security relied on by low-income Americans. Affordable health care for one faces a significant cut, placing it further out of reach of the average citizen. The interventions proposed by Trump to "end the decline" and improve the lives of the large cohort of disgruntled Americans largely defy known economic conduits towards these outcomes.

The world of course sits poised to see if economic growth does materialise in the US, given the global economic impact of the world's largest economy. Emerging economies like South Africa have a significant stake in the success of President Trump's vision for his country. At around 10% of our total trade (lagging trade with Europe at 27% and the rest of Africa at 24% while more or less on a par with our trade with China) the US is not our largest trading partner, but it would matter strategically to not fall out of favour with Washington during the Trump administration. It is, for instance, unlikely that the Trump administration will use soft diplomacy if South Africa is deemed in violation of the eligibility requirements of The African Growth and Opportunity Act (AGOA). Similarly, South Africans' access to, for instance, the products and technology services of American companies like Alphabet, Microsoft, Nvidia and Apple may be at risk, along with other American exports, should these companies come under pressure from Washington to cut ties with countries deemed deserving of punitive interventions. Pretoria's closeness with Moscow, especially, may prove problematic as Trump's pressure on Russia to end the war mounts and also with Teheran, as the denuclearisation contest unfolds.

Growth and opportunity versus uncertainty and disruption

It is overwhelmingly in the best interest of a small, open emerging economy like South Africa if President Trump succeeds and produces, somehow, American jobs, growth and price stability. Given the heightened global risk for disruption, prudent macro policies, like conserving price stability and fiscal discipline, are one way to try and erect some safeguards against external shocks. It may also be a time to consider foreign policy that is as neutral and unambiguously so from the outside as South Africa likes to proclaim.

Financial service firms will need to take a cautious approach over the near term until the impact, size and direction of some of these anticipated changes become clearer for optimal decision making. There are many potential threats to the current business environment but these are sure to be accompanied by opportunities too and firms will need to brace for the former and be prepared to take advantage of the latter as policies are changed and implemented and the level of uncertainty is reduced.

Frank Blackmore

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

Financial Crime

Financial Crime

Fighting the scourge of financial crime

In recent years, South Africa has seen a concerning rise in the scale and complexity of financial crimes being perpetrated, with no signs of slowing down. In its 2024 Annual Crime Statistics Report, the South African Banking Risk Information Centre (SABRIC) reported an estimated loss of R3.3 billion to financial crimes.

The complexity of financial crimes

These financial crimes have evolved over the years with criminal syndicates becoming increasingly creative and adept in their methods to commit crimes. There is a steady increase in the scale of economic crime through criminal syndicates who seem to illegally extract assets or valuable assets and then use money laundering tactics to layer the source of ill-gotten gains. These include predicate crimes of bribery and corruption, fraud schemes, tax evasion, cybercrimes, drug and human trafficking and other organised criminal syndicates involving wildlife poaching and illegal mining.

Moreover, the use of digital currency and assets have become more widespread and with this, we have seen a recent trend that capitalises on the anonymity of these platforms. Criminals use digital currencies to conceal illegal funds, making it difficult for authorities to trace the origins and beneficiaries of such transactions.

Since South Africa's grey listing in February 2023 by the Financial Action Task Force (FATF), and in attempts to achieve its Action Plan, there have been urgent efforts and collaboration amongst local and international role players to effectively remediate the deficiencies identified.

This positive and substantial progress is evidenced by the FATF's announcement in October 2024, of a further nine upgrades to South Africa's Action Plan, with South Africa being deemed to largely or fully addressed sixteen of the twenty-two action items (37 of the 39 applicable FATF Recommendations, including all six core Recommendations). The FATF gave an update just a week ago that four of the six outstanding action items have been upgraded at the conclusion of its latest plenary meetings in Paris, France. South Africa is now deemed to have addressed or largely addressed 20 of the 22 action items in its Action Plan, leaving two items to be addressed in the next reporting period that runs from March 2025 to June 2025. This would enable South Africa to be considered for delisting from the FATF greylist in October 2025.

As part of these collaborative efforts to strengthen South Africa's Anti-Money Laundering (AML) framework and progress the fight against financial crime, South Africa has made key updates to its legislative framework for AML/ counter-terrorist financing (CTF) / counter-proliferation financing (CPF). Policymakers have been mandated to adopt the recommendations from a country risk assessment perspective and relatively cascade it down to the respective Accountable Institutions (AIs) as defined by the Financial Intelligence Centre Act (FICA). There are also currently changes underway on the draft General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Bill, 2024 and the Money Laundering and Terrorist Financing Control Regulations, with the view to ensuring that they clearly address the deficiencies raised by the FATF.

As a result of these legislative developments and the intensified scrutiny by the FIC and supervisory bodies, South African organisations face significant pressure to enhance their financial crime compliance frameworks. Ensuring compliance with these laws may result in increased costs as often this requires significant investment in technology and systems, personnel, and training to meet the obligations. However, these efforts are crucial not only for maintaining regulatory compliance but also for safeguarding the integrity of the financial sector in South Africa.

Companies must take proactive steps to ensure compliance with the evolving AML regulations. This involves not only adhering to the legal requirements but also actively participating in efforts to strengthen their overall AML framework. It's crucial for companies to maintain robust AML practices, conduct regular risk assessments, and keep abreast on the legislative changes and AML trends.

The focus should be on enhancing internal processes and ensuring effective supervision to combat financial crimes effectively. Ongoing training is also vital in keeping up with the everchanging AML and sanctions landscape. By implementing these steps, companies can establish a robust AML framework that not only ensures compliance but safeguards their reputation and minimises the risk of financial crime.

Having said that, it is important to note that the essence of good compliance and governance has a direct correlation to the culture to which each company embeds. A company may have strong financial crime programmes and policies which are functionally embedded; however, the effectiveness of such has to be led by the collaborative efforts of compliance from every stakeholder in a company. There should be a clear culture of wanting to do what is right and good without any compromise.

South Africa still has a way to go in order to exit the grey list and achieving full compliance with the final action items by February 2025, is going to be a challenging exercise. To achieve this, South Africa will need to demonstrate that -

- its AML/CFT supervisory bodies are applying effective, proportionate and dissuasive sanctions for non-compliance to AML/CFT requirements,
- beneficial ownership (BO) information on legal persons and arrangements is adequate, accurate and updated, and authorities have timely access to such, with appropriate remedial actions being applied for non-compliance to transparency requirements of legal persons
- there is a sustained increase in the effective identification of TF activities, and the investigation and prosecutions of serious and complex ML and TF activities.

Remediation of these items is underway, with some of it already evident including the changes to the BO controlling ownership threshold (refer to Public Compliance Communication 59) and the requirement by the Companies and Intellectual Properties Commission for companies to submit BO Declarations alongside their Annual Returns.

It is imperative that companies are aware that the with all these legislative amendments and requirements, comes increased scrutiny, monitoring and enforcement by the FIC and relevant supervisory bodies. Recent year have seen multiple AI's having already being sanctioned for failing to comply with South Africa's AML requirements.

Christy Campbell

Manager
Forensic
T: +27 60 745 6668
E: christy.campbell@kpmg.co.za

Cyber

Cyber

Cyber security in an expanding digital environment

The expanding digital environment—which is emerging, complex, and interconnected with business models and providers—spurs calls for an all-encompassing approach to cybersecurity management. Cybersecurity-related incidents have increased over the past 10 years. South African organisations—particularly financial institutions, healthcare, and government entities—have been victims of targeted cyber-crime incidents or attacks, experienced data breaches, or been forced offline.

Increased Regulatory pressures on Cybersecurity

Regulatory pressures on cybersecurity are increasing globally as governments and organisations strive to protect critical infrastructure and sensitive data. Numerous regulations require organisations to be operationally resilient. A prime example of this regulatory response is the Financial Sector Conduct Authority (FSCA) and Prudential Authority (PA)'s Joint Standard on Cybersecurity and Cyber Resilience, which mandates financial institutions to comply by June 1, 2025.

The minimum requirements and principles set out in the Joint Standard must be implemented to reflect the nature, size, complexity, and risk profile of a financial institution. A risk-based approach is needed to manage cyber risks - this involves mapping out all critical assets, processes, and dependencies, especially those involving third parties.

What is required of Financial Institutions from the Joint Standard?

1. Roles and responsibilities

In the realm of cybersecurity, various roles and responsibilities are essential to safeguard an organisation's digital assets. These roles collectively contribute to a robust cybersecurity framework. The Joint Standard requires that a governing body must exist to serve several objectives—provide oversight of the cyber risk management, establish, implement, and maintain an all-encompassing cybersecurity framework to enable cyber resilience through defined roles and responsibilities.

2. Governance

Institutions must clearly define roles and responsibilities and establish committees for the purpose of exercising oversight of cyber risks. Furthermore, a cyber risk governance and management framework must be established and incorporated into the existing corporate governance and risk management structures and processes to continuously identify, assess, and mitigate cyber risks.

3. Cybersecurity strategy and framework

A comprehensive and robust cybersecurity strategy which is aligned with the overall business strategy must be established and maintained to build a robust security posture that ensures the protection and integrity of critical information assets. The cybersecurity strategy must be reviewed regularly (at least annually) to address emerging threats and align with changes in the business. The Board of directors plays a crucial oversight role in an organisation's cybersecurity strategy to ensure that the initiatives pursued support and protect the organisation's overall business objective.

A cybersecurity framework (aligned with the enterprise risk management framework) must be established to manage cyber risks and regularly assess the organisation's threat profile, considering both internal and external threats, to ensure that it is within the organisation's risk appetite and tolerance levels.

Approved cybersecurity policies, standards, processes, and procedures must exist to manage cyber risks, safeguard IT systems and information assets, and ensure that they are aligned with industry standards and regulatory requirements.

4. Cybersecurity & Cyber resilience fundamentals

The Cybersecurity & Cyber resilience requirements are aligned with the core cybersecurity functions of Identify, Protect, Detect, and Recover as key steps to manage cybersecurity risks and maintain a risk-acceptable cybersecurity posture by performing the following:

- **Identification** - identify and maintain an inventory of critical assets that support key business processes and functions, including those managed by third-party service providers. Assets must be classified in terms of criticality and sensitivity to ensure that the right level of protection, detection, and recovery efforts are implemented.
- **Protection** - implement security controls and best practices to safeguard the organisation's systems and data, through the implementation of controls related to identity and access management, data security and encryption, cryptography, network security and segmentation, secure application and system design and change implementation, and lastly ongoing cybersecurity awareness and training.
- **Detection** – institutions must have capabilities to monitor and identify potential security incidents and cyber events as quickly and accurately as possible. Effective incident detection entails early identification of threats and suspicious activities, prioritisation of critical threats, root cause analysis to implement measures to prevent recurrence as well as drive continuous improvement, and lastly ensure compliance through reporting of security incidents.
- **Response and Recovery** - foundational elements for effective and rapid incident response and recovery to minimise the impact and damage to systems, reducing recovery time and costs must be implemented. Institutions must establish effective policies and processes to improve resilience, support business continuity with defined Response Point Objectives (RPO) and Recovery Time Objectives (RTO), as well as having data backup strategies with supporting plans to perform regular backups and testing to facilitate efficient recovery of IT systems and data in the event of a cyber incident.
- **Incident Response and Management** – institutions must establish incident response and management plans to define the communication, coordination, and response procedures to address cyber threat scenarios.
- **Simulation Exercises** – the effectiveness of the institution's cybersecurity response and recovery capabilities can only be validated through simulation exercises, hence the requirement for institutions to perform regular scenario-based simulation exercises using threat intelligence applicable to the institution's environment.
- **Situational Awareness** – institutions must establish a process to monitor and collect cyber-related threat intelligence into their security operations to build more resilient and adaptive defence systems, foster collaboration, and information sharing with trusted external parties.
- **Vulnerability Assessments** – a process to identify, evaluate, prioritise, and address vulnerabilities in a timely manner; and thereby reducing the risk of cyber-attacks and enhancing overall security posture is required.
- **Penetration Testing** – institutions must conduct penetration testing on all critical IT systems and information assets that are directly accessible from the internet or whenever there are major system changes or upgrades implemented; as a proactive approach to identify security weaknesses, and to obtain an evaluation of its cybersecurity defences.
- **Application security testing** – institutions must conduct security testing on web-based and critical applications during development and implementation to provide insights into the current cyber risks as well as the specific vulnerabilities and potential attack vectors that may be present. Secure coding standards and source code reviews must be adopted. Furthermore, the use and update of third-party and open source must follow established policies and procedures and must be subjected to review and testing prior to implementation.
- **Testing** – financial institutions must regularly test cybersecurity capabilities and security controls to validate the effectiveness of controls. The testing to be performed must follow a risk-based approach taking into consideration the criticality and sensitivity of systems and information assets. It is required that where IT systems or information assets are managed by a third-party service provider, the institution must satisfy itself that the nature and frequency of testing of security controls for the respective IT systems or information assets is commensurate with its own internal requirements.

- **Remediation management** – a remediation process to track and resolve issues identified from the security controls testing or exercises, third-party assessments, and self-assessments as well as findings from internal and external assurance with clear classification, prioritisation of issues, and timeframes for remediation based on risk exposure and severity thereof.
- **Learning and evolving** – institutions must adopt a forward-looking, proactive approach to mitigating against future cyber events and implement mechanisms to learn and evolve to stay abreast of changes in technological and digital advancements which introduce new threats to the environment. Keeping up with the dynamic nature of cyber risks will allow institutions to identify, assess, and manage security threats and vulnerabilities, whilst taking key lessons from cyber incidents that have occurred both internally and externally to advance resilience capabilities.

5. Cybersecurity hygiene practices

Requirements defined relate to:

- Establishing security **access management** policies and procedures, which are reviewed regularly, to enforce control over access rights to IT systems and information while applying principles of "least privilege" and "segregation of duties". Regular review of user access is required to confirm validity and appropriateness of access granted to users. Same level of control must be applied to Third-party service providers and contractors that have access to IT systems and information assets.
- **Privileged Access Management** must be strictly controlled, granted on a need only basis, monitored and reviewed on a regular basis for suspicious or unauthorised activities.
- Implementation of **Multifactor authentication (MFA)** for access to critical system functions, all administrative and privileged accounts and for all user accounts that access systems with sensitive information.
- **Network perimeter defence** with adoption of a "defence in depth" approach to ensure that the network is adequately protected from unauthorised access and disruption.
- **Vulnerability and patch management** process must be implemented to ensure timely application of security patches within a timeframe that aligns with the risks posed by each vulnerability. Compensating controls must be identified where security patches are not available.
- Institutions must define security standards for hardware and software in order to enforce uniform application of **secure configurations** that will minimise the exposure to cyber threats. Standards must be reviewed and updated to ensure relevance and effectiveness.

Malware protection is required to safeguard devices and data from malicious software through regular scanning and anti-malware signature updates.

6. Notification & Regulatory Reporting

Enhanced incident reporting for cyber incidents or information security compromise that have been classified as material incidents, to provide more detailed information about the nature and impact of the incident to the responsible authority in the form and manner determined by the Authorities.

Requirements defined in the Joint Standard are not new; however, it's now insufficient for an organisation to state that it is following best practices; it must prove it through demonstrable compliance. Compliance will require a cultural shift towards cybersecurity – not just a checklist to be completed. Therefore, purely relying on existing frameworks without adapting them to the new regulations can lead to gaps in compliance.

Other noteworthy (emerging) regulation and policy

Emergence of Artificial Intelligence (AI) and Machine Learning:

As AI and other emerging technologies become more prevalent, regulations are being developed to address the associated cybersecurity risks.

The EU AI Act, for instance, aims to regulate the use of AI and create a framework for AI governance and data privacy with objectives to make AI safe and secure for public and commercial use, reduce the risks associated with AI, such as privacy, data misuse and social impacts, keep AI systems under human control and ensure transparency, and address the broader social and environmental impacts of AI.

Similarly, to the way that the General Data Protection Regulation (GDPR) applied to the processing of personal data for EU residents, irrespective of where in the world they are, the EU AI Act applies beyond the borders of the EU. Financial entities and organisations handling large volumes of data face increased scrutiny under the Act, and thus must establish governance frameworks to ensure accuracy and security in their AI applications.

Closer to home, the South African Department of Communications and Digital Technologies has drafted an Artificial Intelligence (AI) Policy Framework. The policy framework is noted as the first step in developing a national AI policy for South Africa. The policy framework emphasises ethical AI, with focus on fairness, transparency, mitigation of biases, as well privacy and data protection. It also highlights the necessity of aligning with global AI governance standards.

Staying ahead of the curve Regulatory pressures are reshaping the cybersecurity landscape, requiring organisations to stay ahead of the curve to ensure compliance and protect against evolving threats. The regulatory requirements demand a deeper integration of cybersecurity practices into the fabric of the organisation and highlighting once again that cyber security is not an IT issue but a business imperative.

Judith Masekwameng

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

Data Privacy

Data Privacy

Breach notifications: bridging the gap between regulation and reality

Doing business in the digital world brings many opportunities and simultaneously exposes businesses to greater risks. This is highlighted in the *WEF Global Risks Perception Survey 2024-2025,* which ranks cyber espionage and warfare among the top 10 risks in both the short term (2 years) and long term (10 years). As organisations continue to place more reliance on technology, companies are fighting a war against relentless cyber attackers who are evolving as fast as technology itself. However, cyber-attacks are just one of the ways a personal information breach can occur—not all breaches need to be so intricate as to disable an organisation. Personal information breaches can also occur from within an organisation - such insider threats may be malicious or simply negligent. Regardless of the intentions of the employee, the ramifications for the organisations and data subjects can be dire.

Regulators globally have recognised the potential harm to data subjects in this digital age where an organisation's data security controls have been compromised. While Information Regulators around the globe insist that organisations implement stringent security controls, they also acknowledge that despite such controls, personal information breaches may still occur.

In South Africa every breach is reportable

Information regulators are also requiring organisations to be transparent about the occurrence of personal information breaches to both the regulator, affected data subjects, and sometimes to the wider public. In South Africa, like many other jurisdictions, the failure to give prescribed notification of a personal information breach amounts to a contravention of the Protection of Personal Information Act 4 of 2013 **("POPIA")**.

Unlike the European Union's General Data Protection Regulation **("GDPR")**, which requires notification to the supervisory authority if a personal data breach is likely to pose a risk to the rights and freedoms of natural persons, POPIA does not prescribe any such threshold. In terms of POPIA, organisations are obliged to report all personal information breaches, regardless of severity.

One concern is that with limited resources, an inundated Information Regulator may find it difficult to prioritise and address the most significant threats effectively, may be delayed in investigating serious personal information breaches (resulting in slower enforcement actions), and delayed guidance to impacted organisations. Perhaps South African legislators should consider amending POPIA to institute a reporting threshold similar to the GDPR, ensuring the Information Regulator's precious time and resources are utilised where it matters most. Another concern, particularly for organisations, is that reporting of insignificant personal data breaches may cause more harm than good – wasting precious resources, bringing about unnecessary regulatory scrutiny and potentially causing unwarranted reputational damage.

However, it is also understood that the legislators may have intended that every breach is reported to both the South African Information Regulator and affected data subjects, to avoid organisations shrugging-off their responsibilities by hiding behind a subjective cloak of "non-materiality". Afterall the consequences for data subjects can be much more dire than an organisation could envisage including identity theft, financial loss, privacy invasion, reputational damage, emotional distress, discrimination, legal consequences, targeted scams and impact on personal relationships.

Identifying a personal information breach is Not always straightforward

Despite every personal information breach being reportable, there is still uncertainty regarding what would constitute a personal information breach in terms of POPIA. "Breach" or "compromise" is not defined in POPIA, instead, whether or not to report a compromise is determined by whether *"there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person"* (section 22(1) POPIA). Since "unauthorised person" is also not defined, the question remains: when is a person considered "unauthorised"? Is it determined by the subjective policies of the organisation, or is there an objective view of when someone ought to be considered "unauthorised"?

It is true that some of the most notable personal information breaches in South Africa involved instances where personal information was accessed or acquired by persons we would objectively consider "unauthorised persons." Examples include the breach suffered by Experian, which exposed the personal information of millions of South Africans and their businesses to fraudsters, and the 3 million South Africans who were impacted after TransUnion's systems were compromised by a hacker.

But what about cases where personal information has not left the safety and security of the organisation itself? Where personal information has been accessed or acquired by employees, who in terms of only internal company policy, are considered "unauthorised". What about a case where an authorised employee (i.e., an employee who has authorised access to personal information) uses the personal information for unauthorised purposes? These types of cases must be common but have not necessarily made headlines in South Africa. Is it because the Information Regulator doesn't consider it a priority in investigating, or potentially because organisations don't consider these breaches reportable in terms of POPIA? If we look to cases abroad, internal personal information breaches would be considered reportable. South African organisations should not presume internal compromises are non-reportable on the basis that the personal information never left the secure premises of the organisation.

Wading through the hazy breach requirements

Once it is determined that a personal information breach has occurred and that notification should be given, organisations are faced with the next challenge of determining the timing of notification of the compromise to the regulator and affected data subjects.

The GDPR requires that the supervisory authority be notified of a breach *"not later than 72 hours after having become aware of it."* Having such a short timeframe within which to give notification may present its own challenges, but POPIA presents a different but equally challenging timing requirement. Section 22(2) of POPIA provides that notification of the breach must be made in writing *"as soon as reasonably possible after the discovery of the compromise."* It is not clear whether reporting is triggered immediately at the time of suspicion of the compromise or after the investigation confirms that a compromise has indeed occurred. Furthermore, there are a number of subjective factors which may delay reporting a compromise, such as the legitimate needs of law enforcement, the measures reasonably necessary to determine the scope of the compromise, and the restoration of the integrity of its information system. Ultimately, what is considered reasonable is subjective and may leave organisations feeling uneasy regarding whether or not the Information Regulator will consider their reporting sufficiently timely.

How to proactively address these gaps in POPIA?

It should be acknowledged that timely identification and notification of a personal information breach is not only a regulatory requirement but a necessity… those actually compromised (the affected data subjects) at least deserve the opportunity to evaluate and mitigate the consequences of the breach of their personal information themselves. It should be borne in mind that the organisation is not always privy to all the information necessary to determine the impact that the breach may have on a data subject – each data subject's circumstances are unique and the impact could be more severe that assessed by an organisation in isolation of the individual facts.

It is imperative that organisations act responsibly by:

- Implementing robust data privacy and information security risk controls (including strict access management controls and controls to allow employees to verify recipients to prevent accidental disclosures by employees).
- Rolling out employee awareness programs informing employees of the importance of applying access management policies in their daily work activities.
- Clearly defining what constitutes a personal information breach in terms of the organisation's policies, having regard to POPIA (despite the potential ambiguity).
- Implementing appropriate processes and procedures to identify any potential personal information breaches quickly, investigating them immediately, and reporting them to Information Regulators and affected data subjects without undue delay.
- Preparing and clearly defining roles and responsibilities in the breach response plan (it is important that stakeholders understand that this is a business risk and not an IT risk in formulating an effective response plan).
- Exercising the response plan (i.e., in simulations) across a variety of possible breach conditions (malicious insider, cyber attack, third-party breach, accidental internal sharing) will also strengthen the muscle memory of the key role players.

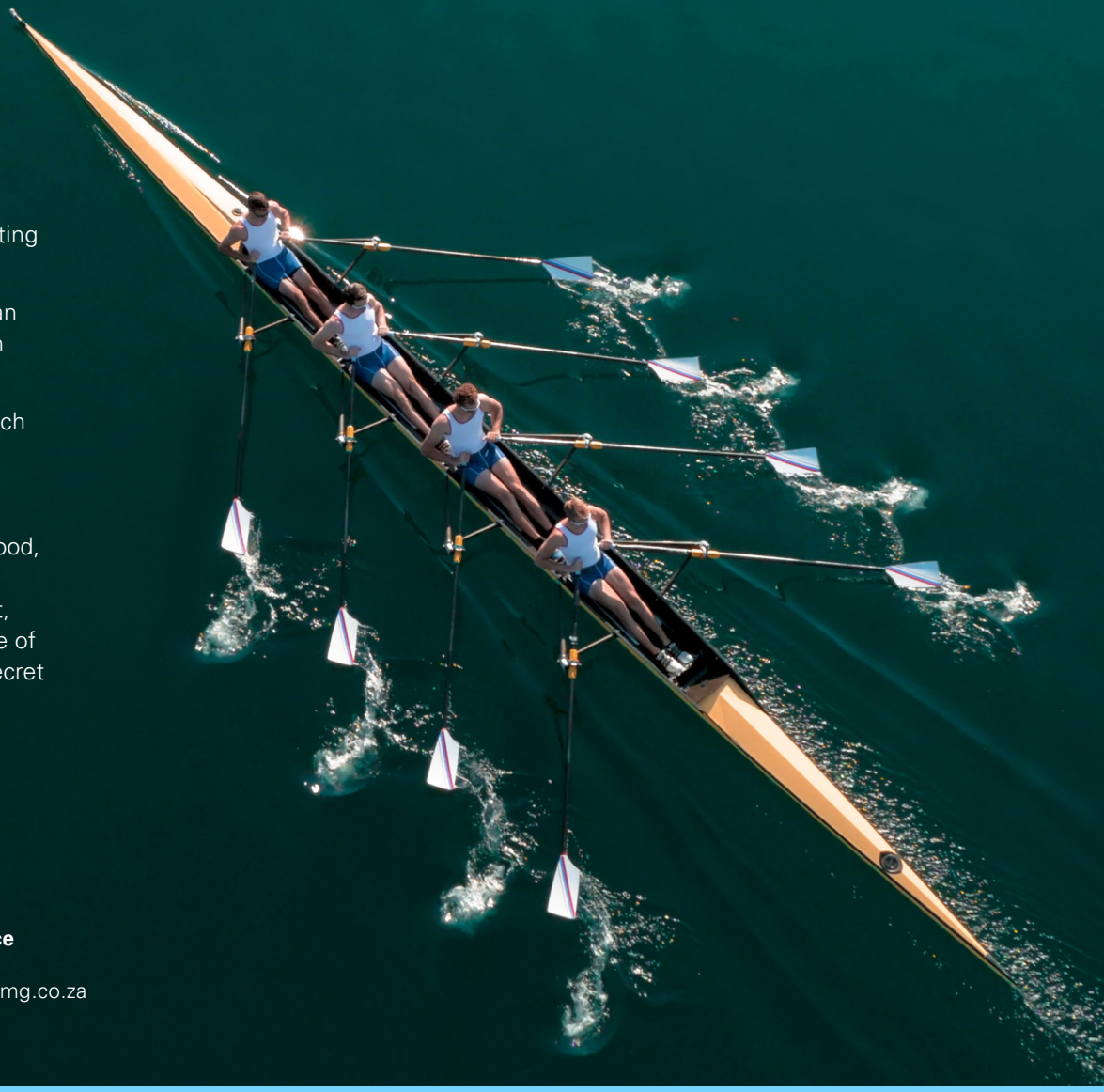
Yes, it is a balancing act—needless notification/reporting may cause more harm than good, especially for an organisation that may suffer embarrassment/reputational damage by reporting a suspected breach that is not, in fact, reportable. However, in cases of doubt, we would implore organisations to err on the side of caution (particularly in the absence of a reporting threshold) and to rather report a personal information breach than keep it secret behind closed doors. After all, the consequences for data subjects can be serious even when the personal information has technically not left the organisation's firewalls.

Nada Ford

Senior Legal Manager
Legal Services
T: +27 72 686 1161
E: nada.ford@kpmg.co.za

Beulah Simpson

Associate Director
KPMG Privacy Practice
T: +27 60 602 3066
E: beulah.simpson@kpmg.co.za



IT Governance

IT Governance

Understanding the technology impact of Joint Standard 1 of 2023

The recently released regulation issued jointly by the Prudential Authority (PA) and the Financial Services Conduct Authority (FSCA), Joint Standard 1 of 2023 ('Joint Standard 1' or the 'the standard'), focusses on IT governance and risk management. The standard is expected to have a significant impact on financial institutions through increased governance requirements that are to be complied with, ultimately by the board of directors (or equivalent governing body).

IT risk management and governance has been receiving increased attention within organisations over the past decade and many of the principles outlined in the standard are not new considerations. The standard, however, now mandates the following requirements which may not always have been high priority:

- enhanced documentation of risks and controls, noting responsible stakeholders;
- being able to report on IT governance to the regulator upon request; and
- obtaining assurance on IT-related governance structures that may have not been subject to assurance previously.
- Tabled below are the key requirements of Joint Standard 1, what this means for financial intuitions (as defined in the standard) and principle questions that the board will need to address:

Requirement	What this means for financial institutions	Questions for the board
1. Enhanced IT governance Ultimately, the board of directors are now directly responsible for ensuring continuous compliance with Joint Standard 1 of 2023. The standard requires financial institutions to develop an IT strategy which aligns to the overall business strategy. In addition, comprehensive IT governance frameworks should align with the organisation's overall corporate governance framework, with the goal of deriving improved value from investment in technology.	To ensure the overall governance frameworks are aligned to IT-specific governance frameworks and ensuring that organisational IT policies and standards are updated to reflect this alignment. Management may face challenges when incorporating IT risks into the overall business risk assessment and applicable governance mechanisms with a single point of accountability.	• Have we ensured that the alignment of general business strategy and governance updates occurs alongside the related IT requirements as part of the annual governance cycle? • Are our business and IT stakeholders convening regularly to ensure alignment and adapting governance frameworks as appropriate? • How often should we, as the board of directors, be assessing compliance with Joint Standard 1 to ensure that compliance is continuously being met, including obtaining periodic representation from key business stakeholders? • What mechanisms do we need to put into place to ensure that any instances of non-compliance with the Joint Standard are reported and remediated in a timely manner?

[1] https://www.fsca.co.za/Notices/Joint%20Standard%201%20of%202023-IT%20Governance%20and%20Risk%20Management%20Requirements.zip

Requirement	What this means for financial institutions	Questions for the board
2. Focus on risk management The standard requires financial institutions to develop an IT risk management framework and regularly conduct risk assessments which aim to identify potential threats and mitigate the risk of these threats materialising. The standard aims to encourage financial institutions to adopt a proactive approach in preventing potential disruptions.	To ensure that an effective risk management framework is managed and linked to risk assessments conducted by management. Management may face challenges in performing risk assessments and implementing responses to these risks in a timely manner. Further challenges include ensuring that controls implemented to effectively mitigate the risk, operate consistently.	• Is our risk register accounting for all IT risks noted in the standard? • Do we have an IT risk management framework that notes the frequency of risk assessments, who is responsible for conducting the risk assessments and how will these risks be managed, reported and documented?
3. Outsourcing and third-party management Financial institutions are urged to identify, assess and manage third-party agreements and associated risks relating to technology providers.	To ensure that IT risks relating to third parties are considered and managed with appropriate mitigations implemented. Management may face challenges in adequately identifying relevant third-party risks by not fully understanding third-party operational environments and may also face challenges in confirming that third-party risks are appropriately addressed, either by the third-party or by the organisation's internal control processes.	• Have we identified all third parties that our organisation engages with and is exposed to? • Have we performed risk assessments over these third parties and ensured that we have identified mitigations prioritised to key third parties? • Have we built risk assessment measures into our contracts with third-parties, where possible?
4. Reporting to the regulatory authority Financial institutions are required to notify the regulatory authority in the event of system failures, malfunction, delay or any disruptive events.	To ensure that any disruptive events are reported to the regulator and that the risk of non-compliance in the event of failure to report, is managed effectively. Management may face difficulty in ensuring that an effective process is in place to identify relevant risk events across the organisation and that it is reported to relevant stakeholders in a timely manner.	• Have we defined the disruptive events that are to be reported to the regulator to ensure compliance? • Is there an established process, including internal stakeholder engagement, to enable reporting in a timely manner? • Do we know which individual or function is tasked with regulatory reporting per our defined definitions of disruptive events?
5. Protection of data In developing an IT strategy, financial institutions are required to incorporate processes that maintain the confidentiality and integrity of data, such as: • identifying and managing the risk associated with financial products; • ensuring backup systems and procedures and business continuity plans are in place; • access control mechanisms; and • maintaining services that are managed by third parties.	• The everchanging nature of technology has resulted in an all-time high of privacy violations and cyber security incidents. The standard places emphasis on the importance of client information and the safeguarding thereof. The standard urges financial institutions to make use of measures to protect client information such as: • access control mechanisms; • encryption of data. IT processes that can be implemented to ensure business continuity include, but are not limited to: • vulnerability assessments; • penetration testing; • incident response plans which delve into root cause analysis and lessons learnt.	• Do we have effective response mechanisms in place relating to data protection, cyber security and resilience and business continuity risks? • How often are these response mechanisms reviewed and reassessed to take into account the new or evolving risk exposures? • Do these responses include the formalisation of specific policies, procedures and effective reporting, as well as clearly defined responsibilities and functions that own the technology risks?

Lessons learnt and insights gained from previous technology-related regulatory implementations

1. Management controls, while possibly adequate, may not always be appropriately evidenced

Our observations indicate that while management may have designed and implemented adequate controls as a response to the identified risk, there is a lack of audit trail to evidence that these controls are consistently performed by management, making it difficult to confirm that controls are operating effectively.

2. Control reporting

To collate the required information and align with relevant stakeholders within an organisation is not always straightforward. As controls serve multiple purposes to address operational, financial reporting or regulatory risks, controls can be at different maturities levels for each business area and therefore may not be well documented and tracked for effectiveness. Reporting on control effectiveness, to cover the requirements of the standard, may prove to be a challenge when controls are maintained across divisions without a uniform reporting structure. Legacy reporting structures will need to be adjusted to allow for reporting at an organisational level in a timely manner.

3. Assurance fatigue

With the technology landscape always receiving heightened levels of attention due to the associated risk, it is of no surprise that multiple streams of assurance may be required by various stakeholders to appropriately manage this risk. This can range from internal assurance (internal audit), external assurance (mandatory external audit or ISAE 3402/SOC engagements for service providers), and focused regulatory audits. This places a resource capacity burden on IT staff and management to provide input to various assurance provides, whilst also maintaining a focus on executing day-to-day tasks required to effectively maintain the IT landscape and operations.

Conclusion

Joint Standard 1 of 2023 reshapes the landscape of IT governance for South African financial institutions. The overall impact on financial institutions will include short-term disruption to day-to-day activities as management embed control and reporting mechanisms to compliment business as usual activities. The long-term benefit will be enhanced insights into the organisation's technology landscape and mitigation of IT related incidents – which ultimately promotes an IT resilient organisation. The integration of IT risk and governance activities as part of an overall risk strategy allows the board to have a holistic view of risks and controls relevant to financial institutions and ultimately ensure compliance.

Ultimately this will allow for a more consistent approach to risk identification, assessment and response across the industry. By embracing technology, managing risks with appropriate controls, and diligently meeting reporting obligations, financial institutions can achieve success in this evolving regulatory environment.

Ashaylan Moodley

Associate Director
Technology Risk
T: +27 82 719 2738
E: ashaylan.moodley@kpmg.co.za

Footnotes/useful links:

[1] Joint Standard 1 of 2023 - Information Technology (IT) Governance and Risk Management Requirements for Financial Institutions

Tax Transformation

Tax Transformation

Managing tax today and transforming tax for tomorrow

In today's rapidly evolving regulatory environment, tax transformation has become a critical consideration for Chief Tax Officers and Heads of Tax within the Financial Services (FS) industry. The increasing demand for tax transparency and comprehensive reporting is reshaping the tax landscape, both globally and locally. As financial services organisations pursue growth, they are often engaged in broader business transformations which includes finance and data management enhancements. However, many are overlooking the imperative of tax transformation. With the changing tax environment, financial institutions recognise that traditional approaches to tax management are no longer sufficient.

Revenue authorities worldwide are proactively leveraging technology to close compliance gaps and enhance revenue collection. Testimonials from tax authorities around the world, already indicates exceeding these tax goals by leveraging digital reporting mechanisms and other technology enhancements. In South Africa, the South Africa Revenue Service (SARS) is implementing strategies to improve indirect tax reporting. These include:

- **Development of VAT Data Models:** To enhance supply chain visibility, SARS is looking at developing sophisticated VAT data models. These models allow for better tracking of goods and services throughout the supply chain, ensuring that VAT is correctly applied and collected at each stage. By analysing this data, authorities can identify discrepancies and potential areas of non-compliance.
- **Digital reporting and e-invoicing mechanisms:** SARS is also considering adopting digital platforms that encompass both digital reporting mechanisms and e-invoicing to enhance real-time data exchange and reporting. The integration of e-invoicing ensures that all transactions are recorded and reported in real-time, granting authorities immediate access to transactional data from accounting systems, with no time for manual interventions. These mechanisms are already proven by more than 70% of regulators around the world as increasing efficiencies and revenue collections.
- **Formulation of the Modern VAT Return:** The modern VAT return is a strategic priority aimed at enhancing the transparency and accuracy of VAT reporting. SARS intends to refine VAT return disclosures by requiring more detailed information and comprehensive analysis to facilitate robust VAT reconciliation validations. By advancing the level of disclosure and analytical rigor in VAT returns, SARS seeks to streamline the compliance process, reduce administrative burdens, and improve the precision of VAT assessments.
- **Pre-Populated VAT Returns:** The abovementioned strategies are facilitating SARS' move toward pre-populated VAT returns, a reality already in place in some African countries, particularly within the financial services sector. This approach not only aligns with international best practices but also positions SARS to better leverage data analytics for enhanced compliance monitoring and risk management. The focus on pre-populated VAT returns underscores a commitment to leveraging technology to simplify taxpayer obligations while ensuring the integrity and accuracy of the VAT system.

In South Africa, the implementation of BEPS Pillar 2 introduces specific challenges related to the recently promulgated Global Minimum Tax (GMT) legislation. This legislation aims to ensure that multinational enterprises (MNEs) pay a minimum level of tax, regardless of where they operate. For South African financial institutions, this means navigating a complex web of global tax rules and ensuring compliance with both local and international requirements. The GMT legislation necessitates meticulous data management to accurately collect and curate hundreds of data points to calculate and report the effective tax rates across different jurisdictions.

The critical role of data

One of the primary data challenges posed by Pillar 2 is the need for comprehensive data aggregation from multiple sources, including financial statements, tax returns, and inter-company transactions. Financial institutions must ensure that data is consistently formatted and standardised to facilitate accurate calculations of the effective tax rate. Additionally, there is a need to reconcile differences in accounting standards and tax regulations across jurisdictions, which requires sophisticated data mapping and transformation processes.

Another significant challenge is the real-time monitoring and updating of tax data to reflect changes in tax laws and rates globally. This requires robust data governance frameworks and advanced analytics capabilities to ensure that the data used in GMT calculations is current and accurate. Furthermore, institutions must implement stringent data security measures to protect sensitive financial information from breaches and unauthorised access. The complexity of calculating the effective tax rate under Pillar 2 also demands enhanced data validation and audit trails to ensure transparency and accountability. Financial institutions must be prepared to provide detailed documentation and evidence to support their tax calculations, which necessitates a high level of data accuracy and integrity.

Overall, the implementation of BEPS Pillar 2 in South Africa presents significant data management challenges for financial institutions, requiring them to invest in advanced data analytics, governance, and security solutions to comply with the GMT legislation effectively.

Despite the unique challenges faced by financial services businesses, a common thread persists: the critical role of data and technology. Insights from KPMG's global and local tax surveys reveal a consistent demand from FS Heads of Tax for deeper business insights, governance, and performance metrics. They are also seeking ways to leverage technology tools to enhance their operations. The key focus areas for FS Heads of Tax include:

- **Value Creation:** FS Heads of Tax must ensure that the tax function is not merely a compliance necessity but a strategic asset that contributes to the organisation's overall value. This involves integrating tax considerations into business planning and decision-making processes. By doing so, the tax function can help identify opportunities for tax savings and incentives, optimize the overall tax position, and support the organisation's growth objectives. In the context of BEPS Pillar 2, value creation also means ensuring that the organisation's global tax strategy aligns with the new minimum tax requirements, thereby avoiding unnecessary tax liabilities and enhancing shareholder value.
- **Risk Mitigation:** FS Heads of Tax must maintain comprehensive visibility over tax compliance across all jurisdictions in which they operate. This involves implementing robust governance frameworks and controls to manage tax risks effectively. By leveraging technology, organisations can enhance their ability to monitor compliance, identify potential risks early, and respond proactively. This is especially important for multinational financial services organisations that must navigate diverse regulatory environments and ensure adherence to the GMT legislation.
- **Cost Efficiency:** Achieving cost efficiency within the tax function is essential, especially as organisations face increasing pressure to optimise resources. FS Heads of Tax should focus on streamlining tax processes, reducing manual interventions, and automating routine tasks. This can be achieved through the adoption of advanced tax technology solutions that enhance operational efficiency and reduce compliance costs. By doing so, the tax function can allocate more resources to strategic activities, such as tax planning and advisory services, thereby adding greater value to the organisation.
- **Data Management and Analytics:** Effective data management and analytics are paramount. FS Heads of Tax must ensure that their organisations have robust data management systems capable of handling complex tax data requirements across multiple jurisdictions. This involves investing in technology that can aggregate, analyse, and report tax data accurately and efficiently. By leveraging data analytics, organisations can gain deeper insights into their tax positions, identify trends, and make informed decisions that align with their strategic objectives.

- **Data Integration and Interoperability:** Ensuring seamless data integration and interoperability across various systems and platforms is crucial for effective tax management. FS Heads of Tax should prioritise the development of integrated data ecosystems that connect disparate data sources and enable a unified view of tax information. This involves adopting standardised data formats and leveraging APIs (Application Programming Interfaces) to facilitate data exchange between systems. In the context of BEPS Pillar 2, integrated data systems enable organisations to efficiently aggregate and analyse tax data from multiple jurisdictions, ensuring compliance and strategic alignment.
- **Tax Technology Skill Development:** As tax technology becomes more sophisticated, developing the necessary skills within the tax function is essential. FS Heads of Tax should focus on upskilling their teams to effectively utilise advanced tax technologies and data analytics tools. This involves providing training programs and resources that enhance technical competencies and foster a culture of continuous learning. By equipping tax professionals with the skills needed to navigate complex tax technologies, organisations can maximise the value of their technology investments and improve the overall effectiveness of the tax function. In the context of BEPS Pillar 2, having a tech-savvy tax team is critical for managing compliance and leveraging data-driven insights.

The need for tax transformation

The rapidly changing regulatory landscape necessitates a comprehensive tax transformation for financial services organisations. As traditional approaches become obsolete, Chief Tax Officers and Heads of Tax must embrace data and technology to navigate complex global tax rules and ensure compliance. By focusing on value creation, risk mitigation, and cost efficiency, tax functions can evolve from mere compliance necessities to strategic assets that contribute to organisational growth. Effective data management, integration, and the development of tax technology skills are crucial for leveraging insights and enhancing operational efficiency.

As financial services undergo broader transformations, harnessing advanced tools and technologies will be pivotal in driving efficiency, ensuring compliance, and aligning with global tax requirements. Ultimately, a proactive and strategic approach to tax transformation will enable financial institutions to thrive in an increasingly demanding tax landscape. Generative AI is a critical strategic priority within the financial services tax sector. The tax function should proactively leverage this technology, working in collaboration with other business units. It is essential to define and evaluate the most effective applications of Generative AI to drive targeted improvements in tax processes and outcomes.

Madelein Van Zyl

Partner
Tax
T: +27 82 718 8810
E: Madelein.vanzyl@kpmg.co.za

Payments

Payments

The Value of South Africa's Payments Ecosystem Modernisation

South Africa's National Payment System (NPS) is undergoing significant transformation, driven by the nine goals of "The National Payment System Framework and Strategy Vision 2025" including the need to enhance financial inclusion, promote competition and innovation, and the adoption of a clear and transparent regulatory and governance framework. As a result, the SARB has launched the Payments Ecosystem Modernisation (PEM) programme that aims to modernise and improve South Africa's payment system. These changes present both strategic challenges and opportunities for financial institutions (banks and non-banks), requiring consideration of investment priorities and operational adjustments.

This article highlights some of the key considerations that financial institutions should contemplate and potentially incorporate into their own payments modernisation journeys based on the perceived impact of the PEM programme.

Overview of the PEM

According to the SARB "The PEM is one of the most significant strategic interventions in the payments ecosystem since the introduction of the SAMOS system and the enactment of the NPS Act nearly 30 years ago." This programme introduces fundamental changes that will reshape the payment landscape across the several components including:

- Establishment and operationalisation of a digital payment infrastructure through the implementation of a public Payments Utility (PPU).
- Implementation of an efficient, cost effective, and more inclusive fast payment system that caters for a range of use cases including person to person, person to business, and government to person, considering lessons from the current PayShap and Real-Time Clearing systems.
- Modernisation of the RTGS system in response to the encouraging competition by allowing access beyond existing participants to use the RTGS infrastructure, while ensuring safety, reliability, and efficiency of the NPS.

Therefore, the PEM programme potentially will require strategic and business model changes in how financial institutions are structured and operate:

Strategic impact of the PEM programme to financial institutions

- Financial institutions need to prepare for the transition to a modern real-time payment infrastructure, requiring significant technological investments but enabling new service offerings and revenue streams.
- The adoption of ISO 20022 message standards necessitates substantial systems updates while enabling enhanced data capabilities and improved automation.
- The introduction of standardised APIs aided by composable architecture and open banking regulation will encourage interoperability and enable new partnership models, though requiring careful management of security and data privacy challenges.

Business model impact of the PEM programme to financial institutions

- Financial institutions should strategically position themselves for increased data sharing and third-party integration, potentially leading to new customer value propositions, revenue models, and partnership opportunities.

- The lowering of barriers to entry particularly in the clearing and settlement environment will introduce new players, requiring established institutions to reassess their value propositions and competitive advantages.
- Enhanced payment capabilities will enable new product development and service differentiation opportunities, particularly in real-time low value electronic payments and value-added services.

A perspective on potential investment priorities and/or considerations

- Technology infrastructure modernisation
    - Modernisation of core payment systems to support real-time processing
    - Implementation of ISO 20022 message standards
    - Development of API management capabilities
    - Enhancement of security and fraud prevention systems enabled by advanced data and analytics capabilities such as the use Artificial Intelligence (AI)
- Target operating morel redesign
    - Process redesign to support faster payment processing
    - Staff training and capability development
    - Risk management framework updates
    - Customer education and support mechanisms

A perspective on the way forward (short- and medium-term focus)

Short-tem focus (0 - 12 months)

- Conduct impact assessment of PEM requirements
- Actively participate in industry working group(s)
- Maintain open dialogue with regulators
- Develop a clear roadmap for technology modernisation
- Prioritise investments based on business impact and regulatory requirements

Medium-term focus (12 - 36 month)

- Engage early with technology partner(s) and vendor(s)
- Identify new revenue opportunities enabled by PEM
- Develop strategies for competing in a future enabled by an open banking payments ecosystem
- Plan for data monetisation opportunities inline with regulatory guidelines and requirements

The future of Payments

The PEM programme represents a fundamental shift in South Africa's payment landscape. While the implementation challenges exist, the programme creates opportunities for financial institutions to modernise their operations, enhance their service offerings, and introduce new revenue streams. Success will require a balanced approach to investment, innovation, and risk management.

Financial institutions that take a proactive approach to PEM implementation, while maintaining focus on customer needs and operational excellence, will be best positioned to thrive in the modernised payment ecosystem. Executive leadership must ensure their organisations have the right strategies, capabilities, and resources to navigate this transformation successfully.

Sources consulted: 1 - SARB Transforming Payments, 2 - The National Payment System Framework and Strategy, KPMG Payments Modernisation Report

Sydney Khumalo

Principal Consultant
Digital Consulting
T: +27 60 976 8263
E: sydney.khumalo@kpmg.co.za

Operational Resilience

Operational Resilience

Redefining Resilience

The Prudential Authority ("PA"), released two directives to banks, one in December 2021 (Directive 10 of 2021) and another in May 2023 (Directive 4 of 2023). These directives provided the principles to be adopted by 31st December 2024. Whilst this was the due date to comply on a "principle-based level" in reference to the Basel Committee on Banking Supervision ("BCBS") white paper on "Principles for Operational Resilience" (released in August 2020), South African banks are still within the early stages of implementation.

South African banks have commenced their Operational Resilience journey with foundational elements such as establishing frameworks and governance to demonstrate the ability to comply and detailing an implementation roadmap which was fit for purpose and in line with the size and complexity of these organisations. Detailed regulations or rules have not yet been released, however, the directives and regulations are likely to evolve in the near future to ensure that the PA is able to define specific requirements and enable a mechanism against which to measure compliance. Whilst the directives apply to banking institutions at present, interest in the value derived from implementing Operational Resilience in related sectors and others is picking up momentum.

Guiding principles for operational resilience

Leading financial services firms have adopted the following guiding principles:

- A top-down led approach to Operational Resilience driven by senior management and the board of directors.
- Embedding an Operational Resilience mindset within the organisation's culture.
- Identify and map out the technology, data, people, processes, third parties, and premises that support IBSs to ensure the end-customer always receives a complete service experience.
- Define threshold tolerances and use "severe but plausible" scenarios to conduct end-to-end testing.
- Develop approaches beyond traditional BCP planning to focus through a business lens on managing disruption.
- Define appropriate escalation paths and decision-making procedures combined with effective and timely communication plans.
- Assume that disruption will occur.

Whilst guiding principles are important to steer the implementation journey, there are some core challenges that organisations are facing.

Whilst guiding principles are important to steer the implementation journey, there are some core challenges that organisations are facing.

Challenge	**Considerations to address**
Lack of clearly defined "tone from the top" messaging in relation to Operational Resilience.	The Board and Senior Management are ultimately accountable for Operational Resilience. Obtaining their buy-in, commitment and support is of paramount importance in ensuring that the roll out is supported, funded, and seen as a top priority.
Lack of consideration to the mindset shift and change management	It's the organisation's people that will be needed to drive successful outcomes and assist in the execution of key activities and initiatives. Many people, including business continuity professionals, are still in the process of understanding what Operational Resilience brings to the table. It is essential that upfront awareness and training is prioritised to ensure employees and key stakeholders "walk the journey together".
Information and institutional knowledge to facilitate the mapping of assets and resources to defined IBSs	Whilst mature organisations may have well documented business process mapping information to support the mapping to assets and resources to IBSs across resilience pillars (technology, people etc.), this information is usually not contained within a single golden source. It is critically important to ensure that the right people are assisting with the mapping exercise and are able to identify assets and resources that support IBSs. Challenges arise when the completed mapping is validated and varying sources of information are then produced which may involve reperforming the exercise, delaying the identification of key gaps and vulnerabilities.
The difference between "perceived harm" and "actual harm" to the customer in the event of a breach of impact tolerance, is not clearly understood.	When setting impact tolerances, it should be emphasised that the "business" must put themselves in the shoes of the customer and ask critical questions such as: - What do stakeholders use this service for and what is the outcome delivered to them? - What are the types of harm that will impact the customer? - What metrics are available to assess impact / harm which result from a service disruption? - Once set, do we have a clear rationale for that impact tolerance threshold?
Unclear ownership of key business services	Business service models differ from organisation to organisation, with many parts of key processes which support the delivery of an IBS, being segregated across varying business units and sometimes even across different sub-entities. Establishing clear ownership for service-based resilience ensures that clear lines of accountability and responsibility exist. Having multiple owners of an IBS from a resilience standpoint is not preferred.

By implementing a realistic strategy for Operational Resilience, tackling challenges from the onset, and ensuring that activities are driven through guiding principles, organisations will be able to experience the following five key areas of benefit:

- Allow better work in a dynamic ecosystem and break down silos between key resilience capability areas (Cyber, IT Continuity, Third-Party Risk Management etc.)
- Generate synergies across strategic, financial, and Operational Resilience
- Reduce operational risks and costs of disruption
- Allocate resources more effectively and efficiently
- Improve supplier and third-party relationships to transform them from "relationship" to "partnership"
- Enhance customer trust and loyalty

Tooling solutions

The granular resource mapping requirements such as mapping services, critical processes and the underlying assets across technology, data, third parties, people, and premises – is a complex data mapping exercise that requires a detailed understanding of the many relationships that exist across an enterprise. Leveraging tooling to support this exercise ensures that mapping is delivered robustly and can be relied upon when it matters most.

Tooling enables firms to accurately map the risks and controls for each asset to the processes and services that they support, highlighting where critical dependencies and vulnerabilities exist and which remedial measures are required. It provides a contextualised, business-informed view of those assets and the risks they pose to the firm and enhances the ability to allocate resilience investment to the assets that need it most.

This business-informed understanding of risk applies across risk domains – third party, cyber, technology, data, insider, premises, energy supply and natural disasters. By contextualising data from each of those risk domains using tooling, specialist teams can collaborate more effectively because they share common metrics and objectives – reducing risk and building resilience across the firms' most critical services and products. It articulates risk in terms that senior management comprehend and, armed with the correct tooling, enables leaders to make defendable, data-informed decisions that stand up to scrutiny when it matters most.

When an incident materialises, quick access to quality data is vital – and so is the ability to interrogate it, exploit it, and surface insights about the firm that will enable it to recover with minimal impact. The correct tooling enables firms to act dynamically during incidents as they unfold, to equip the right people with the data they need to make informed decisions, and to automate burdensome, time-consuming activity so practitioners can focus on strategic, forward-looking activity that will protect the firm, its customers and wider market.

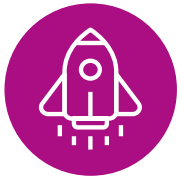
Adapting to the changing environment

By leveraging the power of software, resilience leaders can identify vulnerabilities proactively, mitigate risk before it materialises, and stay ahead of incidents as they unfold. The correct tooling elevates the profile of the resilience function and puts it at the centre of organisational decision making. Tooling should provide a robust data model that acts as the nerve centre of the enterprise – informing firms where they may break, showing which vulnerabilities need prioritisation, and which remedial measures will build resilience where it matters most.

Manesh Purshotam

Senior Manager
Tech Risk
T: +27 72 263 6697
E: manesh.purshotam@kpmg.co.za

Climate and Sustainability



Climate and Sustainability

Africa climate realism vs climate idealism in the Trump era

International developments

The USA had already become the world's leading oil and gas producer during the Biden era. It had been slipping behind the Biden 2030 climate targets to cut climate pollution by up to 66 per cent within a decade. On 5 February 2025, President Donald Trump signed an executive order withdrawing the US from the UN Paris Agreement on climate change and its associated climate goals. President Trump also signed an executive order declaring a national energy emergency that Trump said would unlock untapped oil and gas reserves and increase oil, coal, and gas production. This is part of a broader effort to unwind clean energy which President Trump blames for fuelling inflation. This is just the start of regulatory processes to reverse Biden administration energy policies.

The Paris Accord exit calls into question a host of other US commitments, such as providing billions of dollars in support to poorer nations suffering from unprecedented heat waves, floods, and rising seas. The US is the second-biggest greenhouse gas polluter after China, which is driving up global temperatures. Without the US, the world would fall even further behind the Paris Agreement's goal of limiting the Earth's warming to 1.5 degrees Celsius, a threshold that could accelerate the pace of climate damage. The US withdrawal from global climate goals significantly undermines global decarbonisation and climate finance coordination. The US withdrawal will give China and other competitors a competitive advantage in dominating clean energy manufacturing and innovation.

On 17 January 2025, the US Federal Reserve announced that it had withdrawn its membership from the Network of Central Banks and Supervisors for Greening the Financial System (NGFS), a global coalition of central banks aimed at working together on climate and green finance issues. The US Securities and Exchange Commission is also expected to remove and abandon climate disclosure rules for listed firms.

US and Canadian banks

Four of Canada's biggest lenders announced in February 2025 that they were also withdrawing from the global banking sector climate coalition, joining the six largest US banks. The Canadian banks said in separate statements that they were equipped to work outside the alliance and develop their climate strategies.

US banks are expected to downplay their public commitment to climate initiatives while continuing internal efforts to understand and manage climate risks. One example is Goldman Sachs, which exited from Net Zero Banking Alliances amidst growing political and legal pressure, particularly from red states who argue that Net Zero Banking Alliance membership could violate anti-trust laws. Similarly, BlackRock Vanguard and State Street face lawsuits from 10 red states on similar accounts.

US and Canadian global banks must still comply with other country and regional regulations such as CSRD in Europe and South Africa Climate Change Act, DFFE and SARB regulations. We expect American banks to increasingly aim for minimum compliance in jurisdictions with mandatory climate risk management, reporting and disclosure requirements. US banks may not report, but they already have programs to manage climate risk (i.e., climate scenario analysis and guidance for climate-related financial risk management).

As we advance, US and Canadian banks risk falling behind other global and regional DSIBs and GSIFIs in this area placing them at a competitive disadvantage. Other banks have built up these capabilities and data sets for over ten years and will continue to be better equipped to finance the inevitable transition.

There are potential short-term domestic advantages for US banks distancing themselves from climate commitments but with the long-term risks of falling behind in global competitiveness. There are banks that have taken a very short-term domestic perspective, such as Citibank. These US banks have publicly distanced themselves from net alliances, which has gained them favour with the domestic oil & gas industries. This is expected to lead to some lucrative financing deals in the short term with increasing risk of stranded assets and revaluation risks in the long term.

China

The US and Europe lost the race to China in renewable energy generation, long-distance transmission, nuclear energy, fission energy, critical minerals, AI, robotics, and most critical future technologies. Chinese innovation has reduced the cost of renewable energy well past the inflection point, where renewable energy is now much cheaper than fossil fuels. To realise renewable energy potential will require the redesign of Africa's electricity grids and transmission infrastructure.

The decarbonisation trend in China is so profound that by 2026, China is forecasted to reach peak oil demand before the USA and Europe, with oil consumption expected to decline thereafter gradually. Asia will be responsible for over 80% of global economic growth, with over one billion Asians (mainly China and ASEAN countries) joining the middle class by 2030.

Africa

The evolution of the new multipolar world will profoundly impact Africa, and it will be fundamentally different from recent history and experience. Pre-colonisation, China and India were the world's largest and most developed economies, titles they held for thousands of years. The fast-evolving multipolar world benefits as the world advances. Africa will have increasingly more options and greater bargaining power to fund its economic and social development and climate ambitions.

Most of the world, including China and India, have exploited over 90% of their renewable energy resources. In comparison, Africa has exploited less than 10% of its available hydro-power, solar and other renewable resources. Potential hydro-power is multiples of the total electricity Africa generates annually. With the cost and maintenance of electric vehicles now lower than internal combustion engines, abundant low-cost hydro-power makes Africa's case for reducing the carbon intensity of its energy and transport sector the most compelling globally. Ethiopia and Uganda successfully demonstrated that this can be done with the largest African 6500 MW hydro-power plant at Grand Ethiopian Renaissance Dam (GERD) and Uganda's largest power plant (600MW), Karuma Hydro Power Plant, both completed in 2024. Uganda currently has 20 mini hydro-power projects in the pipeline to more than double electricity generation by the end of 2025, doubling it again by 2030. Ethiopia and Uganda's Renewable energy supply is now over 80% of their energy needs, with it expected to increase to over 90% by 2030 for both countries.

South Africa

The SARB Prudential Authority (PA), in its February 2025 engagement with the financial industry, stated that ESG and Sustainability discussions at international forums had been paused.

The implementation of the South African Climate Change Act is gaining momentum. The Climate Change Act enables the government to legislate national emissions trajectory and targets and allocate sectoral and company carbon budgets. The Minister of Forestry, Fisheries, and the Environment (DFFE) leads the implementation of the Act and coordinates climate change responses across government departments, including the SARB, FSCA and the Ministry of Finance. The DFFE released the draft Emissions Targets (2025 - 2030) Regulations last year, and these are expected to be finalised by June 2025 for implementation and alignment by all sectors, including financial services. The SARB issued guidance last year, which it expects to be implemented and aligned with mandatory Climate Change Act and DFFE regulations. The SARB PA Climate Guidance implementation is mandatory for DSIBS and SIFIs with full compliance expectations by 2028. The Climate Change Act DFFE and SARB Regulations are key requirements for South Africa to access Climate and Sustainable Finance and significantly increase and reduce funding costs.

The six major US banks that withdrew from the climate coalition have significant corporate and investment banking market shares and presence within African countries, including South Africa. These US banks operating in Africa will be driven by short-term fossil fuel self-interest. African countries and financial sectors can expect that US banks will aggressively downplay climate ambitions and aggressively promote in particular the oil industry, in particular to large Pan-African banks.

EU Green Deal

The EU's sustainability reporting and due diligence framework is seen as a major source of regulatory burden. The current US administration opposes the EU Green Deal, particularly the Carbon Border Adjustment Mechanism (CBAM), viewing it as protectionist or a threat to US economic interests. US lawmakers have already stated that the extraterritorial scope amounts to a serious breach of US sovereignty and a direct threat to the global competitiveness of American companies. The US resists the EU's climate goals, undermining global decarbonisation and climate finance coordination. This is straining transatlantic relations and complicating multilateral climate efforts.

The CBAM's negative impact on Africa is more significant as a share of GDP due to the EU being Africa's largest export market and the relatively higher carbon intensity of Africa's exports. CBAM will increase existing inequalities within Africa. Richer and economically developed countries and those that have already made progress in transitioning to a lower-carbon economy will benefit more, leaving the most vulnerable African countries behind. Most, if not all, African countries that oppose CBAM have initiated a WTO trade dispute that received support from the BRICS and most developing countries.

The European Commission is expected to unveil an "Omnibus package" by the end of February 2025 that would modify certain key EU laws on sustainability reporting, but a delay cannot be excluded. The reforms aim to simplify sustainability-related reporting obligations, but much uncertainty remains.

The US government officials and the US Chamber of Commerce are lobbying Brussels to ensure the changes benefit the USA. Whether the EU effort will streamline the laws or a broader rollback such as the push to weaken anti-deforestation rules will be revealed later.

In June 2024, the European Central Bank (ECB) issued stern warnings with a threat of daily fines of up to 5% of revenue to banks and asset managers that were not on track to meet the ECB's 1 January 2025 deadline for factoring climate risk into their business models. All EU SIFI banks and large asset managers have asked for condonation and deadline extensions. At the same time, we have observed that EU implementation of the climate-related regulations has been extended by another 2 years.

On 30 January 2025, the European Insurance and Occupational Pensions Authority (EIOPA) recommended updates to how natural catastrophe risks are accounted for in insurers' standard formula calibrations following a comprehensive reassessment exercise conducted in 2023 and 2024.

Trump, carbon finance and decarbonisation

Climate finance commitments from the US are expected to decline significantly, further exacerbating the climate funding gap for Africa, and developing nations, Africa. It will weaken Europe's ability to lead by example and encourage other developing countries to follow.

The US is a major shareholder in the World Bank, and its withdrawal from the Paris Accord will influence the Bank's climate-related investments. The Trump administration's withdrawal from the Paris Agreement is expected to significantly reduce US contributions to multilateral climate funds managed by the World Bank, such as the Global Environment Facility (GEF).

The US is one of the largest financial contributors to the United Nations Framework Convention on Climate Change (UNFCCC)and its affiliated programs, including the Green Climate Fund (GCF) and other climate-related initiatives. US withdrawal from the UNFCC will create a UN funding gap that will affect the implementation of climate projects in Africa and other developing countries. The UNFCC will have to cut programs, slowing progress on key initiatives like capacity-building and technical support for national climate plans (NDCs) for Africa and other developing countries.

In the past, the UNFCCC relied more heavily on contributions from other major donors, such as the European Union, Japan, and Germany. Due to the weaker economic position, the EU and other developed countries are unlikely to make up for the shortfall and may even reduce their contributions.

In January 2025, Trump also issued an executive order pausing all USAID funding, including climate-related projects. USAID's operations were scaled back, with funding frozen and contracts terminated. This disrupted climate and ESG-related projects and led to layoffs, undermining USAID's ability to support climate goals in vulnerable regions. Under Trump, USAID's priorities have shifted away from climate action toward other areas such as economic development and humanitarian aid. Climate-related work, which had been a growing focus under the Biden administration, was largely terminated. New and future Sustainable and climate-related donor and philanthropic funding in Africa has significantly been reduced, and the impact will become more evident in the months ahead.

The World Bank, UN, and USAID's capacity to continue to support Africa and developing countries with their climate mitigation and adaptation efforts has been reduced significantly. The impact for African climate funding will become more evident in the coming months.

Trump tariffs and carbon markets

Tariffs are expected to result in a stronger US dollar and higher interest rates from inflation, weakening the African country's balance of payments. This will result in increasing foreign debt servicing costs. The local currency cost of serving climate-related projects funded with foreign currency will increase further, reducing the potential number of bankable climate-related projects.

The Trump administration's climate policies and EU tariffs will reduce the demand for carbon credits within the US, hinder the development of international carbon markets and delay progress on scaling carbon markets. Voluntary Carbon markets may provide some continuity, but at a smaller scale than compliance-based systems.

The impact

The impact of the above developments will be felt across the financial services sector in a number of ways:

- **Delayed climate transition and decarbonisation:** The Trump administration's policies will delay the global transition to a low-carbon economy.
- **Climate funding slowdown in Africa:** Trump's climate action and tariffs will slow down and reduce funding for climate-related projects and decarbonisation efforts in Africa and other developing nations.
- **Climate risk management:** Banks, insurers, and asset managers (including the US and Canada) will continue to manage their climate risk, but US and Canadian banks and asset managers are taking advantage of short-term domestic fossil fuel advantages and risk falling behind.
- **Climate risk and opportunity remain**, and the best-prepared African banks and financial institutions will take advantage.
- **Continued cost reductions in renewable energy and innovation** may negate the US slowdown in decarbonisation efforts.
- **Africa substantial gas sector growth until 2030:** Trump's support for oil, coal, and gas will support Africa's natural gas, coal, and oil sectors.
- **Climate public disclosure slowdown:** Expect a global pause in climate-related public disclosure requirements, assurance, or a potential rollback.
- **Increase in climate-related losses:** Failure to adhere to global climate targets, reduced climate and adaptation funding, and increased climate model sophistication will significantly increase actual and forecasted losses.
- **Carbon market slowdown:** Without continued regulatory pressure, companies will lack the financial incentives to invest in credits.

Ben April

Associate Director
Financial Risk Management
T: +27 79 524 9383
E: ben.april@kpmg.co.za

AI Governance

AI Governance

From artificial irrationality to wise artificial governance

A "revolution of common sense"… A "restor[ation] of common sense." These were the words (repeated twice) of Donald Trump that struck a chord with me as I listened to his address at Davos on 23 January 2025[1]. He was arguing that his 2024 election victory was a mandate for pragmatic and straightforward governance, highlighting the need for global policies to support strategic goals and objectives rather than dictate them. Trump underscored his commitment to reducing regulations, cutting taxes, and promoting energy independence as key strategies to restore economic stability and growth.

Love him or hate him, there was something that resonated with business executives globally. To some extent, South African financial services executives, have similarly urged our political- and regulatory elite, to shape regulations and governance as enablers (especially with a large informal economy sector) that safeguard strategic objectives, rather than a pendulum pulling towards sometimes irrational outcomes. There is a growing chorus that feels too much of our financial services regulations chokes and stifles necessary growth. Over-regulation kills.

There is a caveat. The absence of regulations and the flouting of governance can equally lead to systemic risks, particularly when business executives abuse their market-dominant positions to achieve selfish aims. This abuse can manifest in various forms, such as anti-competitive practices, exploitation of consumers, and unethical behavior. Unchecked profiteering destroys individuals and communities. Whilst governance should not stifle innovation nor strategy, it must provide a framework that ensures ethical conduct, fairness, and accountability reigns.

In the context of Artificial Intelligence (AI) governance, this principle becomes even more critical. AI systems have the potential to revolutionise industries, but without proper regulation, they can also lead to unintended- and damaging consequences. AI algorithms can perpetuate biases, invade privacy, and make decisions that lack transparency. Therefore, it is essential to strike a balance between regulating AI to prevent misuse and allowing enough flexibility to foster innovation.

How business leaders embrace governance in terms of the rise of AI will likely shape future outcomes in South Africa. The introduction of provisional AI regulations could too quickly be perceived as not making sense, especially if it's largely just an adoption of first world regulations, notably from Europe. Lack of regulations on AI could result in criticism and blame against the regulator if unfair consumer practices emerge. Both extremes would constitute an irrational response.

Have our regulators been silent on governing AI?

Whilst it might not be apparent, the cluster of financial services regulators incl. the South African Reserve Bank (SARB), the Prudential Authority and the Financial Sector Conduct Authority (FSCA) seem to be working on regulating AI and other emerging technologies. One would have wanted more visible engagements on it, but it's at least on the FSCA's 3-Year Regulation Plan (2024-2027) in which the FSCA indicated it would focus on ensuring that the regulatory framework is robust, aligned with international standards, and flexible enough to meet its legislated objectives. The plan emphasised the need to address emerging risks associated with new and emerging technologies, including AI[2].

[1] https://www.weforum.org/stories/2025/01/davos-2025-special-address-donald-trump-president-united-states/

[2] https://www.fsca.co.za/Regulatory%20Frameworks/Regulatory%20Frameworks%20Documents/2024%20FSCA%203-year%20Regulation%20Plan.pdf

"Although Artificial Intelligence (AI) and Machine Learning (ML) is still largely unexplored by the FSCA, the FSCA acknowledges the potential impact of AI and ML on the financial sector. Exploratory work in relation AI and ML will occur during the course of the next year or two and may result in specific policy recommendations. Notwithstanding this ongoing work, the FSCA, in conjunction with the Prudential Authority, is considering including high-level governance principles relating to the use of AI machine learning by financial institutions into the Joint Standard – Culture and Governance requirements for financial institutions. The FSCA will use the targeted and formal consultation processes to further engage on these topics."

These statements and plans reflect the regulators' commitment to balancing the benefits and risks of AI and other emerging technologies while fostering innovation and protecting consumers.

Waiting for legislated governance is not wise. Any strong leader will recognize that even the organisation he or she leads will require some form of safeguards for AI experiments, AI adoption and advanced AI process implementations. In the meantime therefore, business executives, Chief Risk Officers, and control functions can take various steps to ensure their organisations are guarded against "artificial irrationality".

Global best practice on effective AI governance appears to include at least some of the following elements:

1. Ethical Considerations and Bias Mitigation

- AI systems must adhere to ethical standards to avoid perpetuating biases and discrimination. Financial institutions should implement comprehensive guidelines for ethical AI use, emphasizing transparency, fairness, and accountability. Boards need to take a clear stance on what the common sense standard for their organisations are. This involves:
  - **Bias Mitigation:**
    - Implementing measures to detect and mitigate biases in AI algorithms. Chief Risk Officers will need to build internal team and technology capabilities to independently test for these.
    - Regularly auditing AI models to identify and mitigate biases that could lead to unfair treatment of certain customer groups. External reviews can play a key role.
  - **Transparency:**
    - Ensuring AI decisions are explainable and understandable, thereby fostering trust among stakeholders.
  - **Accountability:**
    - Assigning clear responsibility for AI decisions and establishing mechanisms for addressing grievances related to AI-driven outcomes.
    - Organisations should already be working towards clear first-line, second-line and third-line responsibilities and reporting regarding AI.

2. Data Governance

- Data is the lifeblood of AI. Robust data governance is essential for ensuring the quality, security, and privacy of data used in AI systems. Key aspects include:
  - **Data Privacy:**
    - Ensuring robust data privacy protections to safeguard sensitive information. This should already be well embedded, but the risk exposure increases if AI tools are not properly implemented with the necessary security safeguards
  - **Data Quality Management:**
    - Implementing processes to ensure data accuracy, completeness, and consistency.
  - **Privacy and Security:**
    - Adhering to data protection regulations such as POPI (and GDPR if applicable) and implementing robust cybersecurity measures to safeguard sensitive information.
  - **Data Lineage and Provenance:**
    - Tracking the origins and transformations of data to ensure its integrity and reliability.

3. Model Governance

- Model governance involves overseeing the development, deployment, and monitoring of AI models to ensure they operate as intended. This includes:
  - **Model Validation:**
    - Conducting rigorous testing and validation of AI models before deployment to ensure their accuracy and reliability.
  - **Continuous Monitoring:**
    - Implementing ongoing monitoring mechanisms to detect and address performance degradation or anomalies in AI models.
    - Control functions will increasingly be expected to express opinions and views on AI models.
  - **Version Control:**
    - Maintaining a repository of different model versions and their respective performance metrics to facilitate comparisons and track improvements.

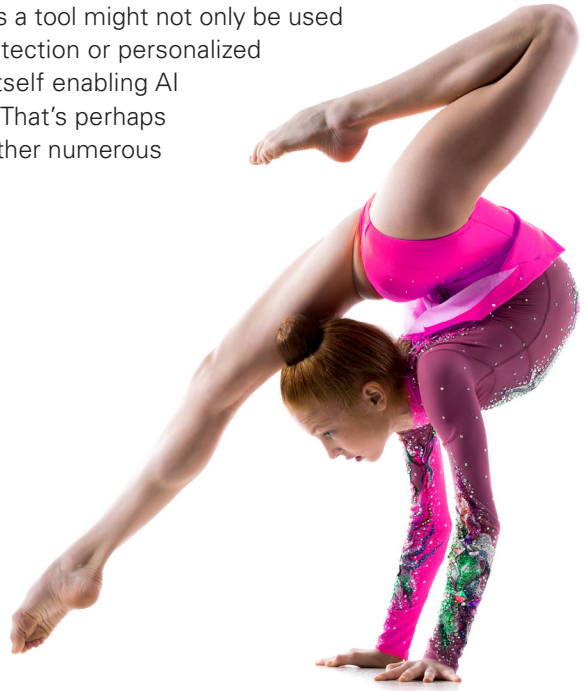
4. Regulatory Compliance

- Financial institutions will likely have to navigate a complex landscape of regulations governing AI use. Ensuring compliance readiness involves:
  - **Regulatory Awareness**:
    - Staying informed about new and evolving regulations and guidelines related to AI and financial services. Global regulatory developments give us a good reference point so long in South Africa.
  - **Compliance Audits:**
    - Conducting regular audits to ensure AI systems adhere to regulatory requirements.
  - **Reporting and Documentation:**
    - Maintaining comprehensive documentation of AI processes, decisions, and compliance measures to facilitate regulatory reporting and inspections.

5. Risk Management

- AI introduces new risks that must be proactively managed. Financial institutions should integrate AI risk management into their broader risk management frameworks. This involves:
  - **Risk Identification:**
    - Identifying potential risks associated with AI, including operational, reputational, and legal risks.
  - **Risk Assessment:**
    - Evaluating the likelihood and impact of identified risks to prioritize mitigation efforts.
  - **Risk Mitigation:**
    - Implementing strategies to mitigate AI-related risks, such as establishing fail-safes and redundancy measures.

When strategically approached, AI as a tool might not only be used for predictive analytics and fraud detection or personalized customer experiences, but also in itself enabling AI governance- and risk management. That's perhaps the strength to unlock from all the other numerous benefits AI offers.



The power of responsible AI

By adopting these governance measures, organisations can harness the power of AI responsibly, ensuring it serves as a tool for positive change and guarding against irrationality, whilst allowing progress towards "artificial integration" in organisations. AI governance can play a leading role in enabling strategic growth drivers for financial services in South Africa.

AI offers transformative potential for financial services, but its integration must be managed wisely to avoid artificial irrationality. Governance is the cornerstone of rational AI, ensuring that AI systems operate ethically, transparently, and in compliance with regulations. By focusing on ethical considerations, data governance, model governance, regulatory compliance, and risk management, financial institutions can harness AI's power while safeguarding their integrity and reputation.

By prioritizing AI governance, financial services firms can pave the way for wise artificial integration that drives innovation, efficiency, and sustainable growth.

Whilst Trump may be entertaining interesting futuristic or alternative concepts in governance, it's obvious Artificial Intelligence (AI) Governance in 2025 will become the linchpin that ensures AI systems function as intended and align with organisational goals and regulatory requirements. As AI becomes more deeply integrated into various business processes, there needs to be a dedicated focus to ensure it operates rationally and responsibly. Perhaps this will lead to a Chief Artificial Risk Officer role, separate from the current Chief Risk Officer role, in years to come given its pervasive use and unique features and business impacts.

Marius Botha

Partner
Financial Risk Management: Actuarial
T: +27 72 123 7194
E: marius.botha@kpmg.co.za

Case Study: AI Governance in Action

To illustrate the importance of AI governance, consider the case of a leading insurer that implemented an AI-driven pricing algorithm on its online quotation tool. The system initially showed promising results, with improved accuracy and efficiency in assessing insurance risk factors. However, a lack of robust governance led to significant issues:

Bias Detection Failure: The system disproportionately assigned higher premiums to minority applicants due to biases in the training data socio-economic factors applied. In particular, the AI-based model component on retention which determines lapse probabilities based on a variety of different data (e.g., personal attributes such as gender, age, income etc) and initiated lapse-prevention measures materially loaded premiums rate for a segment of customers that has the same profile as another similar segment.

Transparency Issues: Customers and regulators raised concerns about the opaque decision-making process of the AI model.

Regulatory Non-Compliance: The firm faced regulatory scrutiny for failing to adhere to data protection and fairness standards.

As a result, the firm suffered reputational damage and stakeholder trust waned.


KPMG
Subscribe to KPMG's weekly FinWatch newsletter
A weekly compilation of financial services regulatory updates from Southern Africa, the broader African continent and abroad, directly to your mailbox