KPMG

Ten key regulatory challenges of 2026

The long and winding road

kpmg.co.za

Introduction

On behalf of KPMG Africa's Regulatory Centre of Excellence, I am delighted to share the sixth edition of our annual flagship publication, *The Ten Key Regulatory Challenges of 2026*.

The theme for this year's edition is "The Long and Winding Road". While not specifically referencing the hit song written by Paul McCartney for the Beatles in 1970, many of our readers will agree that it has indeed been a long and winding road for the financial services sector. National Treasury published the *Red Book* on South Africa's financial services regulatory reform, titled *A Safer Financial Sector to Serve South Africa Better, in 2011*. Since then, we have witnessed significant transformation in how the sector is regulated; from the implementation of the Twin Peaks model of regulation in South Africa, to more recently, a number of countries on the continent successfully exiting the FATF grey list and the introduction of increased capital requirements for banks. Yet, when reflecting on our previous editions, many of the core themes remain consistent.

For the first time, this year's edition provides a truly continental perspective on financial services regulation, incorporating insights with specialist views from across Africa, together with a dedicated article on the ZARONIA transition for our South African readers.

Enjoy the read and I hope that you are humming the melody of the long and winding road in your head.

- **Geopolitical Risk**
- **Financial Crime**
- **Third Party Risk Management**
- **Climate and Sustainability**
- **Data Privacy**
- **Capital Agility**
- **Cyber Security**
- **Artificial Intelligence**
- **Cross Border Payments**
- **Lean Regulatory Risk Management**
- **Plus 1 BONUS Article Zaronia Transition**

Michelle Dubois

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

Ten key regulatory challenges of 2026

Geopolitical Risk

Geopolitical Risk

Improving economic fundamentals under a cloud of geopolitical risk

This time last year, the global community was apprehensive, expecting upheaval to emanate from the United States. It came quickly, in February 2025, when the US administration announced their first round of tariffs on both allied and non-allied countries, exceeding predictions of political and economic turbulence across the globe. The announcement of subsequent *Liberation Day* tariffs in April 2025 injected much frustration and uncertainty into international relations at both the political and economy level, risking destabilising the increasingly fragile world order. Over the short term, asset prices declined and country representatives scrambled to achieve an audience with the White House in efforts to negotiate more favourable trade terms with the United States.

Trump tariffs and transition

For many years, societies in the western world had developed deeply entrenched dependencies on US goods and services, ranging from consumer goods to defence systems and equipment, from technology to financial systems and entertainment. This embeddedness rendered western partners particularly tied but also exposed to (shifts in) the norms, values and ideals espoused by the United States. Historically, based on shared values and beliefs, this arrangement has remained benign and mutually beneficial in a rules-based geopolitical order. The imposition of tariffs by the Trump administration on its allies however signalled the US' departure from a values-based system, making the perils of the entrenched power imbalance very clear. Previous allies have been forced to now focus on ways to reduce the threats posed by the concentration of power held by the United States. In global politics, it has led to a rethink of global alliances. On an economic level, global supply chains and trade partners are reassessed, all while attempting to appear neutral or allied to the current administration of the United States. Actions or stances perceived as non-conciliatory may invite potentially costly retaliation.

The result of tariff and other trade negotiations with the US during the first half of 2025 came into effect in August 2025. Less severe than the near-prohibitive tariff schedule proposed in April, some much-needed tariff certainty supported a more growth-oriented second half of the year for both the global economy, Africa and South Africa. This is despite South Africa's inability to negotiate a reduction in the country's *Liberation Day* tariff, which remains the highest in Africa along with Libya and Algeria at 30 percent, while much of the rest of Africa faces rates of half of this amount if any.

Even so, South Africa was able to make progress with respect to its economic performance and global standing through some strategic interventions.

Formal interventions to address weaknesses in its mechanisms of oversight over money laundering and terrorism financing allowed South Africa's delisting from the *Financial Action Task Force's (FATF)* greylist, which reduces the compliance requirements for financial interactions with South African entities. Besides also allowing a greater variety of investment alternatives access to South African securities, the reduction in compliance costs should grow the volume and value of transactions and therefore benefit South African trade and ultimately growth.

The impact of lower inflation

The encouraging statements made in November by the Minister of Finance in the medium-term budget policy statement (MTBPS) served as a further tailwind to the South African economy. The Minister reiterated government's commitment to fiscal consolidation and announced the reduction of the national inflation target to 3 percent, within a narrowed target range of 2 to 4 percent. Fiscal consolidation reinforces trust in the fiscal integrity of the country in an era of widely reported misuse of public funds and entails the commitment that tax revenues will be directed towards service delivery and growth initiatives. Lowering the inflation target offers multiple, significant benefits for the country; broad macroeconomic benefits include a stronger exchange rate and lower interest rates.

Lower inflation further benefits growth through stimulating domestic savings and investment, improves the competitiveness of South African production, and yields fiscal benefits in the form of reducing debt services costs, which would free up fiscal resources. Lower inflation also contributes to domestic distributional equality through less erosion of incomes and asset value for its citizens and preserving purchasing power of all South Africans.

The above-mentioned initiatives contributed to an upgrade of South Africa's sovereign credit risk rating towards the end of the year. In addition, the rand was able to appreciate by 18 percent against the US dollar over the course of 2025. These improvements coupled with the continued resilience of the South African economy over the year have led most analysts to predict a real economic growth rate for 2025 of more than 1 percent. Although a notable improvement over the decade-long average wreal growth of 0.7 percent, significantly faster growth would be required to meet SA's social and development objectives.

The year ahead should aim to build on the gains made in 2025 to achieve the higher economic growth required to begin to address the high unemployment and poverty levels in South Africa. By all accounts, the global environment should be conducive to achieving this end. Inflation has slowed and allowed central banks to reduce interest rate with more such reductions to come in 2026. Lower interest rates would mean greater demand for credit from both consumers and businesses, which would raise consumption and investment spending and ultimately lead to higher levels of economic growth globally. The same is true for South Africa. The combination of a reduction in the inflation target and the expected low inflation rate making room for further interest rate reductions through 2026, which would support greater consumer and investment spending domestically. Combined with ongoing initiatives aimed at expanding the capacity of the economy, specifically the structural reforms aimed at improving the electricity and logistics infrastructure through the introduction of private investment and (in some instances) management, South Africa has the opportunity in 2026 to make progress in terms of economic growth, which may create multiplier benefits over the medium to longer term.

Global headwinds will have an impact on the local economy

The optimistic outlook is subject to a caveat that the current global environment faces several potential risks besides the ongoing wars in Ukraine and the Middle East. Most notably, shifting alliances and potential hostilities create geopolitical risks that can disrupt the global economic environment significantly. Near the top of the list of such risks is the US administration's intention to gain control of Greenland in defiance of NATO allies and much of the world. Several scenarios may unfold from this standoff: from diplomatic hostilities, to punitive trade wars and, although currently unlikely, potentially armed conflict to achieve the US annexation of Greenland. The global impacts of the scenarios vary but the latter, in particular, would be very disruptive, giving rise to global inflation, lower economic growth, deepening fiscal constraints and even snowballing of the conflict should other NATO countries come to Greenland's defence. It may also create the opportunity for China to move on occupying Taiwan and would also be supportive of Russia's annexation of parts of the Ukraine. A further potential risk could result from the removal of former Venezuelan president Maduro and what this could mean for the leaders of other sovereign nations that the US administration view as problematic or a threat to US national security.

"According to the Central Bank of West African States (BCEAO), the annual inflation rate dropped to 2.3% in March 2025 from 3.7% in December 2024."

"Annual consumer price inflation as measured by the Consumer Price Index (CPI) was 4.5 per cent in Kenya in December 2025, indicating a stable fiscal environment and moderate price increases in food, beverages, fuel and transport."

– Frank Blackmore, KPMG Lead Economist

Pretoria's closeness with Beijing, Moscow and Tehran may prove problematic and contradictory to South Africa's declared foreign policy of neutrality and nonalignment unless managed more diplomatically than has been the case to date. In this challenging geopolitical environment, many countries demonstrate an understanding that the welfare of the citizens of their own countries is best served by an inward focus and a non-provocative diplomatic position. It is in South Africa's interest to sharpen the focus on what can be achieved domestically to enable greater economic growth and prosperity. Improving the quality of governance deserves high priority. This would include creating a more efficient and effective public service, addressing corruption and mismanagement, and the removal of bureaucracy holding back the growth and development of small and medium businesses. This should go some way to lower the actual and perceived costs of doing business in South Africa and to attract both foreign direct investment and investment by domestic businesses.

Emerging, small, open economies like South Africa have a significant stake in the success of the Trump administration's economic vision for his country. Our trade with the US amounts to just under 10 percent of our total trade, on a par with our trade with China. While lagging our trade with Europe at 27 percent and the rest of Africa at 24 percent, trade with the US remains strategic and falling out of favour with Washington during the Trump administration will be costly. The Trump administration will not use soft diplomacy if South Africa is deemed in violation of the eligibility requirements of *The African Growth and Opportunity Act* (AGOA) and will simply exclude South Africa from the benefits of unrestricted access to US markets. Similarly, South Africans' access to, for instance, the products and technology services of American companies from Ford and McDonalds to technology giants like Alphabet, Microsoft, Nvidia and Apple may also be at risk, should these companies come under pressure from Washington to cut ties with countries deemed deserving of punitive interventions.

Positioning the economy to harness mutually beneficial gains

South Africa will do well to leverage the expected improvements in the global and local economy to pursue its domestic goals of economic growth and reducing unemployment and poverty in a focused manner. This will lay valuable groundwork for future economic opportunities. At the same time, it should plan precautionary to mitigate the potentially costly fallout that may result from any one of many uncertain geopolitical events occurring while avoiding diplomatic stances that may invite harmful and unnecessary downside for South African citizens.

Financial services firms overall stand to gain from the general expected improvement in the economic and business environment in 2026 brought on by the low inflationary environment along with the expected further reductions in interest rates and additional structural improvements and the tailwinds that these should provide the South African economy. However, businesses should also proceed cautiously and take into account the many geopolitical risks that may cause a range of more challenging business scenarios, from a moderate probability of lower economic growth caused by minor political and economic shocks to a reasonable probability of continued rising operating costs and even the low probability of potentially disruptive restricted access to business-critical software and technology under severe scenarios. It would be prudent for most businesses to develop strategies that address some of the more likely scenarios and identify opportunities and make plans to mitigate threats for these. This scenario planning will allow the business to pivot more quickly to the rules of the game they may face through 2026, allowing them to remain on track with the core business strategies and maximise value creation for their stakeholders.

Frank Blackmore

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

Key takeaways

Three actions financial services firms should take in 2026

- Scenario planning in a world of ever-changing geopolitical risks for countries and businesses alike will help cope with the vicissitudes resulting from these and create the best chance of success for their economies.
- The economic benefits of delisting from the Financial Action Task Force (FATF) greylist are clear from the example above and every effort should be made for countries like Kenya to ensure this delisting.
- Consistent foreign policy based on underlying values should be implemented to allow the most beneficial relations within the global economy, especially for countries with long-term growth and development ambitions.

Financial Crime

Financial Crime

The call for collaboration of public and private partnerships is more urgent than ever.

A perpetual risk landscape

Financial crimes, often referred to as economic crimes in academia, have evolved into a global threat with significant economic consequences. The financial crimes regime has shifted from being a responsibility of law enforcement agencies alone, to one that calls for a rather more urgent intervention by more professionals and more roles with foresight to address. The risk management profession has navigated its focus more to enterprise-wide risk management which has a huge aspect of regulatory compliance embedded.

Traditionally, compliance and other assurance providing functions such as Internal Audit and corporate governance, were the main characters in the fight against financial crimes. In light of this, the challenges that face financial crimes compliance are rarely about professional expertise, and more about ensuring the right expertise and capabilities are put into context, to work homogenously. The World Economic Forum (WEF) Global Risks 2026 Report has identified crime and illicit economic activity as a risk that will continue to be active in the next 2-10 years. Although ranked slightly lower as the years progress, the success of dropping this risk completely, will require the collective efforts of public-private partnerships to curb financial crimes.

A global view of financial crimes

The global view of financial crimes is very alarming, according to the Nasdaq Global Financial Crimes 2025 Report. Global financial crimes account for 2-5 percent of global GDP. These illicit flows of money (in and outside) the economy, distorts markets, continue to destabilise economies and mostly fuel inequality. Financial crimes expand beyond Money Laundering, Counter Terrorist and Proliferation Financing (ML/CT&PF).

Globally, the flow of illicit funds accounts for 3.1 trillion USD which are laundered through various financial and non-financial institutions. Businesses should therefore be more aware of the predicate offences which enable the proceeds of crimes. Corruption, cybercrime, tax evasion, drug trafficking, terrorism financing, environmental and other organised crimes, still generate the largest proceeds which are laundered and brought back into the economy. From the 3.1 trillion USD, Nasdaq reports that 1.47 trillion USD (47 percent) originates from such crimes. This is followed by the most overlooked predicate offence, drug trafficking, which largely aids the laundering of money. Drug trafficking contributes a total of 782.9 billion USD (25 percent) to the global total illicit flows.

It is very difficult to decipher financial crimes without unpacking the impact fraud has in the orchestration of financial crimes. It is reported that illicit funds that affect the global economy, due to fraud is 485.6 billion USD (15 percent). The human element of financial crimes is also overlooked as businesses are often of the view that there is little to no impact to them.

The uncomfortable truth is that everyone is affected by financial crimes as the illicit funds go through the same economy in which we operate. The same illicit funds are kept circulating in financial services until there are no traces of the predicate offences. The same money flows through investments, acquisitions, and injected back into the economy to sustain lives. Having said that, human trafficking and wildlife trafficking are still as dangerous as financial crimes. Nasdaq's report further highlights that globally, human and wildlife trafficking also rank as large contributors to illicit flows, with over 346.7 billion USD (11 percent).

Emerging financial crimes

'Deep fakes' that emerge from the usage of Artificial Intelligence have taken fraud to a new level. Customer due diligence has become difficult to conduct due to unreliable sources and deep fakes which impacts compliance. This challenge aligns closely with the misinformation and disinformation risks highlighted in the WEF Global Risk Report.

Interestingly, financial crimes such as trade-based financial crimes are still very much overlooked. The trade (both buying and selling) of illicit goods has emerged as a fast-growing financial crime, that ultimately leads to money laundering. The illicit activities in tobacco and cigarettes, alcohol, fuel and fuel adulteration, counterfeiting, illegal mining, and the smuggling of gold and other minerals, are forms of trade-based financial crimes that not only affect the users of counterfeit goods, but the capital collection reforms revenue authorities aim to achieve. These types of financial crimes will negatively affect taxes and business revenues. The ripple effects of such financial crimes are dire to the economy and individual businesses.

Africa and its unwavering resilience!

Africa truly stands at a pivotal moment. With intentional action and sustained commitment, the continent has a unique opportunity to strengthen its global standing and economic credibility.

The exit of several West and Southern Africa countries from the Financial Action Task Force (FATF) Grey List in October 2025, marked a significant milestone. Countries such as Burkina Faso, Mozambique, South Africa and Nigeria have subsequently seen their removal from the European Union's High-Risk Third-Party Country Jurisdiction list. This is an indication that the world is watching and the more we work together, as a continent, the more this translates into positive visibility globally. Admittedly, victory can only last as long as sustainable reforms are embedded.

The Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) has highlighted key financial crimes in West Africa being largely related to the predicate offences of banking fraud, romance scams and the usage of complex structures to hide proceeds of crimes. GIABA and its member states have also taken steps to introduce updates to the West Africa AML/CFT landscape focused on intensifying regional oversight and enhancing regulatory frameworks, to combat evolving financial crimes. From a West Africa perspective, Ghana gears up for its 2026 Mutual Evaluation (followed by Senegal in 2027) to ensure that their AML/CFT controls are in place.

South Africa, on the other hand, is also gearing up for its next 2026/2027 FATF Mutual Evaluation which will commence in mid-2026. The common deficiencies relating to prosecution or lack thereof will certainly be the focal point of this year's evaluation for South Africa.

"The exit of the Financial Action Task Force (FATF) Grey list in October 2025 of countries in West and Southern Africa has been deemed a great reward and a steer in the right direction for making Africa attractive."

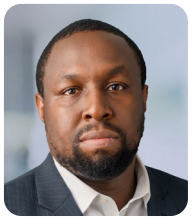
"The exit of Burkina Faso, Mozambique, South Africa and Nigeria from the Financial Action Task Force (FATF) Grey List in October 2025, coupled with Uganda's earlier exit in February 2024, marked a significant milestone. The subsequent removal of these countries from the European Union's High-Risk Third-Party Country Jurisdiction list has been deemed a great reward."

– Lydia Kariuki, Associate Director, Quality & Risk Management, Kenya.

We have largely seen how possible it is to collectively succeed if we are truly intentional. Regulators, authorities, supervisors, businesses, and professionals (both financial and non-financial) ought to make it their business to collectively fight financial crimes. Such partnerships will positively aid the gathering of the right intelligence (data) to enable businesses to make informed decisions and contribute effectively to the broader fight against financial crime.

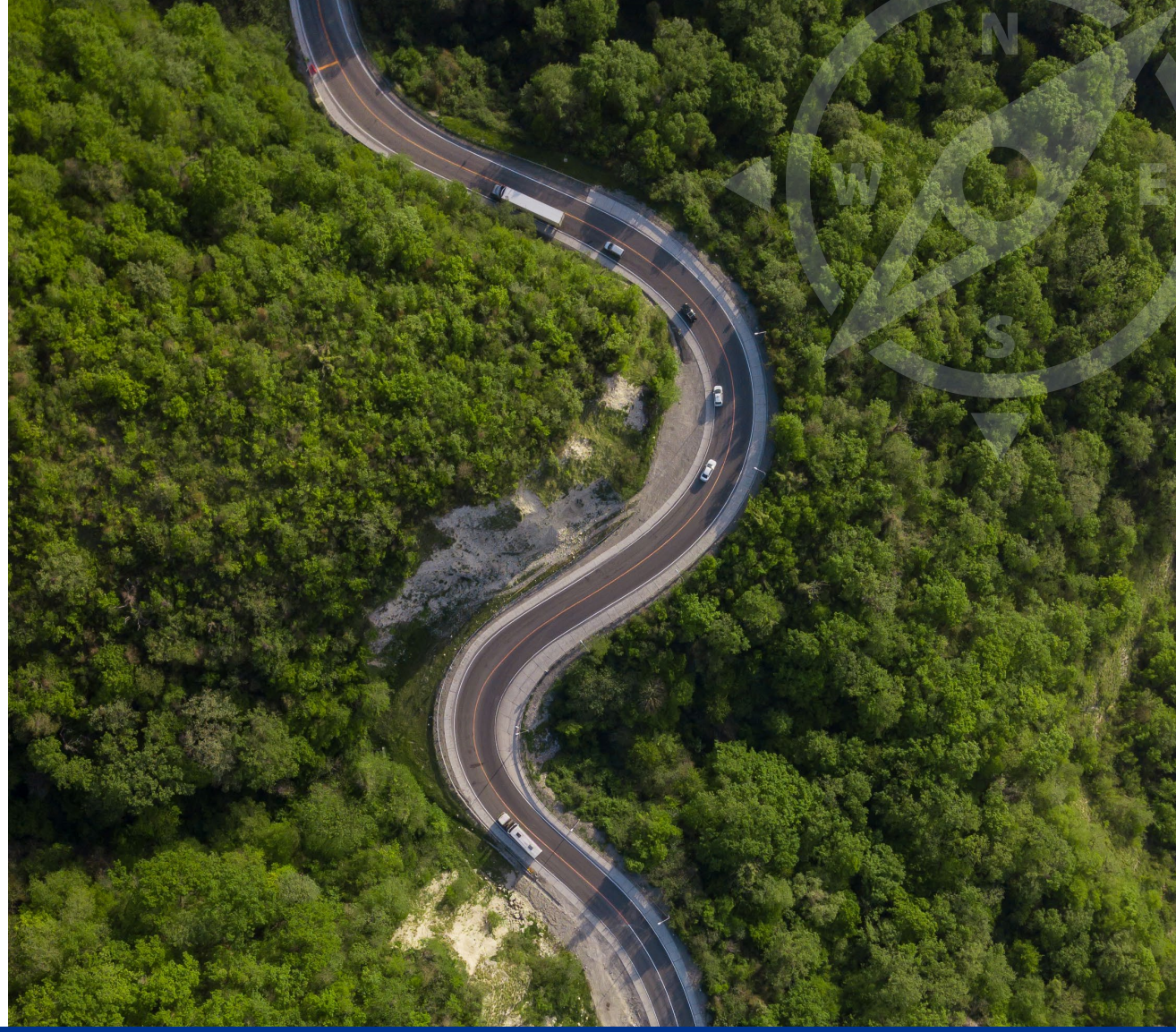
Lebogang Thobakgale

Associate Director
AML Compliance Officer
KPMG South Africa
T: +27 77 602 4307
E: lebogang.thobakgale@kpmg.co.za



Kamsi Atuchukwu

Manager
KPMG Nigeria
T: +23 41 271 8955
E: kamsi.atuchukwu@kpmg.co.za



Key takeaways

Three actions financial services firms should take in 2026

- Be prepared for more regulatory changes that will affect business operations. For example the South African General Laws of AML/CFT Amendment Bill seeks to strengthen intelligence collection, expand due diligence obligations, beneficial ownership enforcement, and the potential introduction of lifestyle audits for higher-risk individuals and entities.
- Various upcoming Mutual Evaluations across Africa (including South Africa) conducted by FATF or regional bodies will potentially influence investment flows, market confidence, and cross-border operations. Grey-listing introduces uncertainty into risk models and portfolio allocations.
- Apply a stricter risk-based approach. Curbing the risk of financial crime can no longer be an isolated function. If financial crimes are not viewed as a 'hot topic' in risk committee deliberations, then businesses may be overlooking risks that directly affect profit-making ability, reputation and long-term sustainability.

Third Party Risk Management

Third Party Risk Management

Extending an organisation's risk management responsibilities beyond its own boundaries

In an increasingly interconnected economy, South Africa's financial institutions do not operate in isolation. They rely on a vast and complex ecosystem of third parties – from cloud service providers and software vendors to payment processors, data analytics firms, and business process outsourcers to operate. While some suppliers have established robust risk and business resilience processes, others are less mature. If proper due diligence is not performed during supplier onboarding, a financial institution could face a significant amount of risk.

These risks manifest across the following categories;

- **Operational risks**, such as service disruptions or failures due to a vendor's poor performance or inability to provide these goods and services
- **Cybersecurity and data privacy risks**, where sensitive information entrusted to a third party becomes vulnerable to breaches or misuse. Cyber-security and data privacy are becoming essential topics for the C-suite. 81% of CEOs interviewed in KPMG's CEO Banking Outlook believe that Cyber-security and data privacy is a top negative contributor to impact growth[1]
- **Compliance and regulatory risks**, arising from a third party's failure to adhere to relevant laws, industry standards, or contractual obligations, potentially leading to fines or legal action
- **Reputational risks**, where a third party's unethical conduct or service failures can damage the organisation's brand and customer trust; and
- **Financial risks**, encompassing unexpected costs, contractual disputes, or the financial impact of a third-party incident. Effectively identifying, assessing, and mitigating these diverse risks is crucial for maintaining business continuity, protecting assets, and preserving stakeholder confidence
- **ESG risks**, considering the potential for an organisation's long-term viability and success to be negatively impacted by environmental, social, and governance (ESG) factors.

Third Party Risk Management is vital because it extends an organisation's risk management responsibilities beyond its own boundaries.

The imperative of TPRM in financial services

The importance of robust TPRM for financial institutions stems from several critical factors:

1. Intensifying Regulatory Scrutiny:

The South African Prudential Authority (PA) designated "Third-party risk management" as its official 2025 "flavour-of-the-year" topic. This means it is a specific, heightened area of supervisory focus for all regulated financial institutions[2]. The PA recognises that failure when dealing with a critical third party can have systemic implications, impacting market stability, consumer protection, and the operational resilience of the financial system. Directives and guidance increasingly mandate comprehensive due diligence, continuous monitoring, and robust contractual arrangements for all third-party engagements, particularly those deemed critical.

1 KPMG (2024) KPMG 2024 Banking CEO Outlook. Available at: https://kpmg.com/xx/en/our-insights/value-creation/kpmg-2024-banking-ceo-outlook.html (Accessed: 27 November 2025).

2 South African Reserve Bank (2025) *Prudential Communication 3 of 2025: Flavour of the Year – Mutual Banks*. South African Reserve Bank. Available at: https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2025/Prudential%20Communication%203%20of%2025_%20Flavour%20of%20the%20year_Mutual_Banks.pdf (Accessed: 27 November 2025).

2. Interconnectedness and Supply Chain Complexity:

Financial institutions are deeply embedded in intricate supply chains. A single service, such as a core banking platform or a trading system, might rely on dozens of underlying third and fourth party providers. This creates a "domino effect" where a vulnerability or failure at one point in the chain can cascade, disrupting critical business functions across multiple institutions. Understanding and managing this complexity is paramount to maintaining operational continuity.

3. Data Protection and Cybersecurity:

Financial services firms handle vast amounts of highly sensitive data, including personally identifiable information (PII), financial records, and proprietary business intelligence. When this data is shared with or processed by third parties, the risk of a data breach or cyber-attack multiplies. Regulators and customers alike demand assurance that this data is protected, regardless of who holds it. Effective TPRM includes rigorous assessment of a third party's cybersecurity posture, data governance, and incident response capabilities.

4. Operational Resilience:

A key focus for financial regulators today is operational resilience – the ability of firms to prevent, adapt to, respond to, recover from, and learn from operational disruptions. Third parties often provide critical services that underpin a firm's operational resilience. A disruption at a key vendor can directly impair a financial institution's ability to deliver essential services to its customers. TPRM is therefore integral to identifying critical third parties, assessing their resilience, and ensuring appropriate contingency plans have been established and tested.

5. Reputational and Financial Impact:

The consequences of a third-party failure can be severe. A data breach, service outage, or ethical lapse by a vendor can lead to significant financial losses (fines, remediation costs, lost revenue), severe reputational damage, and a loss of customer trust. In an era of instant communication, negative news travels fast, making proactive risk management essential for safeguarding a firm's brand and market position.

TPRM is no longer a back-office function; it is a front-and-center strategic concern that directly impacts a financial institution's ability to meet regulatory obligations, protect its assets, and maintain its license to operate.

How can firms improve when managing third party risks?

To better understand and effectively manage Third-Party Risk Management (TPRM), Financial Services (FS) firms should focus on several key areas. This involves a combination of strategic alignment, process maturity and technological adoption.

"Nigeria's Central Bank (CBN) is increasingly emphasising third-party risk management. Its Risk-Based Cybersecurity Framework, which requires banks and payment service providers to establish robust controls for vendor due diligence, monitoring, and contractual oversight. These guidelines reflect CBN's broader push to strengthen operational resilience and protect the financial sector from vulnerabilities introduced by third-party service providers'.

Nigeria's recent delisting from the FATF grey list has been partly attributed to its commitment to adequately regulate the Designated Non-Financial Businesses and Professions (DNFBP) sector. A key focus is ensuring that DNFBPs identify their third parties and monitor their activities effectively.

These regulatory developments place a renewed responsibility on organisations in Nigeria to implement strong TPRM practices."

– Tomi Adepoji, Partner KPMG Nigeria

"Third-party risk management in East Africa is becoming increasingly important as regulators strengthen expectations around cybersecurity, data protection, and outsourcing across the financial sector. Although Kenya, Uganda, and Tanzania emphasise risk-based oversight through ICT and operational resilience guidelines, the region's regulatory frameworks remain largely principles-driven, placing responsibility on organisations to build robust internal TPRM programmes."

– Daniel Karuga, Partner KPMG Kenya

These TPRM elements, actions, and benefits outline a practical roadmap for managing third party risks effectively.

TPRM Element	Action	Benefit
Conduct a Comprehensive TPRM Maturity Assessment	Evaluate current TPRM program against industry best practices, regulatory expectations, and leading frameworks.	This helps identify gaps in policies, processes, technology, and governance, providing a clear roadmap for improvement. It moves firms beyond a reactive approach to a proactive, risk-based strategy.
Map Third-Party Ecosystem and Criticality:	Create a complete inventory of all third parties, including fourth and fifth parties where possible. Crucially, assess the criticality of each third party to the firm's operations, regulatory obligations, and customer service delivery.	Understanding which third parties are truly critical allows firms to prioritise resources, apply appropriate levels of due diligence and monitoring, and focus on areas that pose the greatest potential impact.
Align TPRM with Enterprise Risk Management (ERM):	Integrate TPRM into the broader ERM framework. This means ensuring that third-party risks are identified, assessed, and reported using the same methodologies and risk appetite statements as other enterprise risks.	Prevents TPRM from operating in a silo, provides a holistic view of risk across the organisation, and ensures that senior leadership has a comprehensive understanding of the firm's overall risk exposure and appetite.
Enhance Due Diligence and Ongoing Monitoring:	Move beyond once-off assessments. Implement robust, risk-tiered due diligence processes that cover financial health, cybersecurity, data privacy, operational resilience, compliance, and ESG factors. Establish continuous monitoring mechanisms for critical third parties, leveraging automated tools, where possible.	Provides real-time insights into third-party performance and risk posture, allowing for timely intervention and adaptation to changing risk landscapes.
Strengthen Contractual Governance	Ensure contracts with third parties clearly define service levels, performance metrics, audit rights, data protection requirements, incident response protocols, and termination clauses. Regularly review and update these contracts.	Establishes clear expectations, allocates responsibilities, and provides legal recourse in case of non-performance or breaches.
Invest in Technology and Automation	Explore and implement Vendor Risk Management (VRM) platforms and other automation tools. These can streamline workflows, centralise documentation, automate assessments, facilitate reporting, and provide dashboards for risk visibility.	Increases efficiency, reduces manual errors, improves data accuracy, and frees up risk professionals to focus on higher-value analysis and strategic oversight.
Foster a Strong Risk Culture and Training	Educate employees across all relevant departments (procurement, legal, IT, business units, risk) on their roles and responsibilities in TPRM. Promote a culture where third-party risk is everyone's concern and responsibility.	Ensures consistent application of TPRM policies, raises awareness of potential risks, and empowers employees to identify and escalate issues proactively.
Develop Robust Incident Response and Exit Strategies	Create clear plans for how to respond to incidents involving third parties (e.g., data breaches, service outages). Also, develop comprehensive exit strategies for critical third parties, outlining how services would be transitioned or brought in-house if a relationship ends.	Minimises the impact of adverse events and ensures business continuity, even when a critical third-party relationship is terminated

By systematically addressing these areas, financial services firms can move towards a more mature, effective, and resilient TPRM program that not only meets regulatory expectations but also supports their strategic objectives and promote stakeholders expectations.

Martine Botha

Senior Manager
ESG Advisory
KPMG South Africa
T: +27 63 792 6567
E: martine.botha@kpmg.co.za

Key takeaways

- Conduct a comprehensive TPRM maturity assessment to identify gaps and align with regulatory expectations.
- Implement continuous monitoring and robust due diligence for critical third parties, focusing on cybersecurity, compliance, and operational resilience.
- Invest in technology and automation to streamline vendor risk management and improve real-time visibility of risks.

Climate and Sustainability

Climate and Sustainability

Navigating the climate challenge

Introduction

The escalating climate crisis poses a formidable, multifaceted challenge to global financial stability, with the Southern African Development Community (SADC) positioned on the front lines of this threat. The region's economies, deeply intertwined with climate-sensitive sectors such as agriculture, mining, and tourism, face a heightened vulnerability to both the acute physical impacts of a changing climate and the profound transitional shifts required to move towards a low-carbon future. For African financial institutions, banks, insurers, asset managers and pension funds, which have significant operational footprints across SADC and Sub-Saharan Africa, navigating this complex and rapidly evolving risk landscape is no longer a matter of corporate social responsibility. However, it has become a core business imperative, central to their long-term viability and success.

Climate Change Act 2024

The Climate Change Act No. 22 of 2024 provides the legal framework for South Africa's transition to a low-carbon, climate-resilient economy. The Act establishes a mandatory carbon budgeting system for high-emitting entities, requires greenhouse gas mitigation plans, and introduces significant penalties for non-compliance.

Climate risks

Climate-related risks manifest in two principal forms: physical risks arising from acute, event-driven hazards (such as cyclones and floods) and chronic, longer-term shifts in climate patterns (such as rising sea levels and persistent droughts); and transition risks stemming from societal and economic adjustments toward a low-carbon economy. For financial institutions operating in the Africa region, both categories present material and immediate challenges. Physical risks threaten to disrupt business operations, devalue physical collateral, and impair borrowers' ability to service their debts. Transition risks, meanwhile, create significant uncertainty about the future viability of established business models in carbon-intensive sectors, exposing financial institutions to the risk of stranded assets and market repricing events. Effectively understanding, managing, and mitigating these interconnected risks requires a sophisticated, forward-looking, and deeply integrated approach that embeds climate considerations into every facet of financial institutions operations, from high-level corporate strategy and governance to granular credit underwriting and capital adequacy planning.

Climate Litigation is emerging as a fast-rising risk from regulatory enforcement and stakeholder litigation—over 2900 climate-related cases globally, with banks targeted for financing emissions, greenwashing, and poor disclosures. Key South African Cases that include significant rulings are *Earthlife Africa Johannesburg v. Minister of Environmental Affairs (Thabametsi; Sustaining The Wild Coast NPC v. Minister of Mineral Resources (Shell oil exploration); and the Youth-led #CancelCoal case*. South African litigation cases commonly aim to block new coal-fired power plants, fossil fuel exploration, and challenge policies deemed inconsistent with limiting global warming to 1,5 degrees Celsius. These cases rely on Section 24 of the Constitution (environmental rights), aiming to protect against climate harms.

Africa is experiencing a rapidly widening climate insurance gap, with less catastrophic losses covered despite increasing climate-related disasters. High vulnerability, low insurance penetration and rising reinsurance costs leave communities and governments financially exposed, while the insurance industry faces challenges from intensifying risks.

Climate related risk impact on financial statements

Impact	Credit Risk	Assets and Operations	Regulatory Capital	Liquidity & Funding	Litigation and Insurance
Balance Sheet	**Collateral devaluation** from physical damage.	**Stranded Asset Risk** Fossil fuel exposures may face abrupt repricing, leading to "stranded" assets.	**Risk-Weighted Assets increase,** straining Capital Adequacy Ratios.	**Liquidity Buffer Depletion** from unexpected credit line drawdowns and deposit withdrawals.	**Insurable Gap Increase** Decrease in assets covered by insurance protection.
Income Statement	**Higher Expected Credit Losses (ECL) and Impairments.**	**Costs increase** for new risk infrastructure, data, and specialised climate skills. **Increase in Litigation Costs and Regulatory Fines.**	**Margin Compression** Higher regulatory capital and non-banking competition may squeeze net interest margins in carbon-intensive sectors.	**Borrowing costs increase** from ratings downgrades.	**Regulatory enforcement costs.** **Stakeholder litigation.** **Uninsured assets** backing mortgages or loans lose value, **increasing potential impairments and write-offs.**

The regulatory imperative: SARB's guidance on climate risk

The imperative for robust, transparent, and comprehensive climate risk management frameworks within the financial services sector has been unequivocally established by regulatory bodies worldwide. In South Africa, the Prudential Authority of the SARB has taken a proactive stance, issuing comprehensive guidance notes that underscore the urgent need for FIs to integrate climate-related risks into their core governance structures, risk management processes, and strategic planning cycles [1, 2]. This guidance emphasises a holistic, integrated approach, urging FIs to move beyond treating climate change as a peripheral or reputational issue and to recognise its potential to materially affect all traditional risk categories, including credit, market, operational, and liquidity risks.

A key pillar of this evolving regulatory framework is the pronounced emphasis on forward-looking assessments. Financial services firms should conduct detailed transition planning and utilise sophisticated scenario analysis to test the resilience of their business models and balance sheets against a range of plausible climate futures. This proactive stance is essential for identifying and mitigating potential vulnerabilities before they crystallise into significant financial losses. Concurrently, the global push for standardised, high-quality climate-related financial disclosures—spearheaded by influential frameworks such as the Task Force on Climate-related Financial Disclosures (TCFD) and the new standards from the International Financial Reporting Standards (IFRS) Foundation—has further amplified the call for greater transparency. Adequate disclosure is now viewed as a critical tool for promoting market discipline, enhancing financial stability, and enabling informed decision-making by investors, regulators, and other stakeholders.

Governance and board-level responsibility

The Board of Directors bears the ultimate responsibility for overseeing the firm's management of climate-related risks and opportunities. This responsibility requires active engagement in establishing clear governance structures, ensuring that the appropriate skills and competencies are in place within the organisation, and maintaining regular, rigorous oversight of climate-related strategies and risk management practices.

Firms are required to disclose how their governance structures facilitate the identification, assessment, and management of climate risks, including detailing the specific roles and responsibilities of board committees and senior management-level positions dedicated to climate risk oversight. The Board must ensure that climate-related risks are appropriately integrated into the firm's overarching risk appetite framework and that management is equipped with the necessary resources and authority to implement effective mitigation and adaptation strategies.

1 South African Reserve Bank. (2025). Guidance Note G3/2025: Guidance on Climate-related Disclosures for Banks. Pretoria: South African Reserve Bank.

2 South African Reserve Bank. (2024).Guidance Note G2/2024: Guidance on climate-related governance and risk practices for banks. Pretoria: South African Reserve Bank.

Comparison of climate related risk management and disclosure requirements

The SARB has provided detailed guidance on disclosures, which aligns with international best practices. The following table compares the key disclosure requirements outlined in the G3-2025 and G2-2024 guidance notes, providing a clear overview of regulatory expectations for South African banks.

Sectoral vulnerabilities and systemic implications

The African continent is already experiencing the profound and often devastating impacts of climate change, including recurring droughts, floods, and extreme weather events that disrupt economies and livelihoods. In South Africa, a SARB Working Paper highlighted the critical spatial dynamics of these shocks, demonstrating how climate events in one country can have significant, often immediate, spillover effects on neighbouring nations through shared resources, trade linkages, and regional infrastructure[3]. These shocks have a disproportionate impact on key economic sectors, creating a complex and interconnected web of risks for banks with exposure to the region. The financial cost of climate-related disasters in Southern Africa is already estimated at over US$10 billion annually, a figure expected to rise, contributing to increased poverty and economic instability.

Disclosure Category	G2-2024: Guidance on climate-related governance and risk practices	G3-2025: Guidance Note on Climate-related Disclosures
Governance	• The board is responsible for oversight and management of climate risks. • The Board may delegate to management but must monitor delegated functions. • Recommends establishing an internal climate risk committee or expanding existing ones.	• Disclose governance practices, processes, controls, and procedures for overseeing climate-related risks and opportunities. • Detail the Board's oversight responsibilities, management's role, and the assignment of responsibilities throughout the organisation.
Strategy	• Integrate climate-related risks into business strategy and financial planning processes over the short, medium, and long term. • The Board and senior management are to identify material climate-related risks and incorporate them into the bank's risk profile and policies.	• Disclose the current and anticipated effects of material climate-related risks and opportunities on the bank's business model, strategy, and financial planning over the short, medium, and long term. • Explain how the bank uses climate-related scenario analysis to inform its strategic and financial planning.
Risk Management	• Adopt an integrated approach to climate risk management, • Embed climate risk within risk frameworks under traditional risk categories such as credit, market, operational, and liquidity risks.	• Disclose the bank's processes for identifying, assessing, prioritising, and monitoring climate-related risks. • Describe how these processes are integrated into the bank's overall risk management framework.
Metrics and Targets	• Risk management function must develop appropriate quantitative and qualitative methods and metrics to monitor progress against its strategy and risk appetite. • Metrics must relate to climate-related transition risks, physical risks, and climate-related opportunities.	• Disclose the metrics and targets used to assess and manage relevant climate-related risks and opportunities. • Disclosure includes metrics related to climate-related transition risks, physical risks, and climate-related opportunities.
Transition Planning	• Recommends banks undertake transition planning in proportion to their size, business model, and complexity, • Compile transition plans as part of climate risk management.	• Disclose information about the bank's transition plan, including key assumptions and dependencies.
ICAAP	• Requirement for banks to document and explain in their ICAAP documentation to SARB PA: • Methodology used to identify, assess, and manage climate-related risks. • Details of scenario analysis and stress tests, which must include climate shocks • Impact on internal capital adequacy	• Not a disclosure requirement.

[3] Mazviona, B., Bayai, I., & Mashamba, T. (2026).The spatial dynamics of climate shock impacts in SADC: a focus on selected economic sectors. South African Reserve Bank Working Paper Series, WP/26/01.

[4] SADC Banking Association. (n.d.).SADC-RTGS. Retrieved from https://sadcbanking.org/

[5] Masunda, S. M. (2025). Impact Of Climate Risk On Financial Sector Stability Of The Selected Sadc Countries. Preprints.org.

A roadmap for the future

The SARB's climate related Guidance Notes establish clear expectations, creating a roadmap for how financial services firms should manage and disclose climate-related risks. A proactive and coordinated approach to climate risk management is not merely a prudential imperative—it is essential for ensuring the long-term stability and prosperity of the financial system and the economies it serves.

By implementing robust governance structures, integrating climate considerations into strategic planning, developing comprehensive risk management processes, and establishing meaningful metrics and targets, banks can build resilience into their operations and portfolios.

Transparent disclosure will enable investors, regulators, and the public to assess the adequacy of climate risk management and make informed decisions.

The financial services firms which successfully navigate this transition, managing their climate risks while financing the African continent's shift toward a low-carbon economy, will be best positioned to thrive in the years ahead.

Ben April

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

Key takeaways

- Establish robust governance and enhance board-level expertise.Formally defining the roles and responsibilities of the Board and its committees in overseeing climate-related risks and opportunities, implementing training programs to bridge any knowledge gaps. Appointing a Chief Sustainability Officer or an equivalent senior executive with a direct reporting line to the CEO or the Board can ensure that climate considerations are embedded at the highest level of strategic decision-making.
- Integrate climate risk into the enterprise risk management framework: Update risk appetite statements to include climate risk, develop methodologies to identify climate risk as a driver of traditional risk types (credit, market, operational), and embed climate factors into credit underwriting and portfolio management processes.
- Conduct a comprehensive climate risk assessment and scenario analysis.
- Develop a comprehensive data strategy to address significant gaps in climate-related data. This includes identifying sources for client-level data (such as greenhouse gas finance emissions) and physical risk data for asset locations. Concurrently, develop a set of specific Key Risk Indicators (KRIs) to monitor climate risk exposures and track progress against their climate-related targets.
- Develop transition pathways and target metrics for the short, medium, and long term.

Data Privacy

Data Privacy

Navigating data privacy in an evolving regulatory landscape

In recent years, the adoption of generative AI ("Gen AI") has become a strategic imperative for forward-thinking organisations. The question is no longer whether to embrace this technology, but rather when and how to do so effectively. When implemented thoughtfully, Gen AI is an invaluable tool which offers significant opportunities to drive operational efficiencies, automate routine processes and unlock innovative solutions to complex business challenges.

As organisations integrate Gen AI into their business plans, they face a rapidly evolving and often fragmented regulatory landscape. On the African continent, the way forward is not always clear, as there is not always comprehensive legislation which specifically regulates the adoption of AI tools.

However, that does not mean that there is no guidance provided to African organisations. Whilst there are significant regulatory gaps relating to the ethical use, accountability and transparency of AI systems, existing legislation such as the Protection of Personal Information Act ("POPIA") in South Africa, the Data Protection Act, 2019 in Kenya, the Data Protection Act, 2012 (Act 843) and the Cybersecurity Act, 2020 (Act 1038) in Ghana for instance can be used to assist in navigating some of the compliance related questions.

Understanding the origin of data

When exploring key data privacy principles with Gen AI, we need to understand that Gen AI relies on vast datasets to train an algorithm which infers outputs. The algorithm generates an output in response to a query from a user (the input). Therefore, the quality of the dataset is central to its effective functioning.

Every time a query is input into an AI model, this query becomes data, which is added to the existing dataset. The more queries entered, the more data the AI model has to process the new query and therefore potentially refine the output. This is what we know as 'machine learning'. Using accurate datasets, especially where they contain personal data, is a fundamental aspect of understanding an organisation's data privacy obligation when using Gen AI. Every organisation which uses Gen AI needs to have a holistic understanding of where the data which is used to train the model is obtained from, if personal data is included in the data, and what efforts have been made to ensure that the dataset is reliable. Organisations can address this by undertaking a data mapping exercise to assist in their understanding of where the data is sourced from, where it flows through and where it exits the organisation. This is one of the first steps in undertaking a review of Gen AI in relation to your privacy compliance programme.

A lawful basis for processing personal data

Organisations embarking on the journey to deploy Gen AI tools have a responsibility to remain accountable to their customers and their employees, whose personal data has been entrusted to them. As responsible parties, they must establish a lawful basis for processing personal data within their Gen AI tool and be transparent to their data subjects about how and why their personal data is processed. When data subjects are unaware that their personal data is being used in Gen AI tools, it prevents them from being able to exercise their rights and have control over their personal data. A privacy notice drafted in clear and plain language, setting out what categories of personal data are ingested, how it is used, how long it is retained for, and what their rights are, is essential to deliver this messaging to data subjects.

The important role of data privacy assessments

Data privacy impact assessments conducted at the design stage of the Gen AI tool act as a critical tool in assisting organisations to identify, assess and mitigate against any privacy risks which may arise. It assists with, amongst other things, ensuring that only the minimum personal data necessary is collected, an adequate lawful basis for processing has been established, that privacy notices clearly articulate the reasons for processing personal data, the personal data being processed remains accurate and up-to-date, and that there are adequate security controls in place. Data privacy impact assessments assist organisations to remain compliant with data protection regulations, safeguard individuals' personal data and build trust with their data subjects by demonstrating a proactive and risk-based approach to responsible AI deployment.

Following on from this, organisations should be aware that input queries which are used to train the AI model are kept by the system for future training. If a query contains personal data, it could be kept indefinitely if not managed properly, which creates significant risk from a data breach perspective. Thinking about retention periods and what processes an organisation takes to ensure that personal data is properly disposed of should form part of the data privacy impact assessment considerations.

Data privacy regulatory considerations

In South Africa, POPIA states that business cannot use personal data to make decisions which result in legal consequences for data subjects, where that decision is solely arrived at on the basis of automated processing of personal data ("automated decision making"). For example by feeding a potential client's personal data to a Gen AI model to determine whether they should be extended a line of credit and then denies that person credit solely on the basis of the AI output. A way in which organisations can avoid being non-compliant with POPIA is by having a human review the decision made by a Gen AI tool who is able to confirm or override the decision before it is implemented will assist in avoiding potential biases, hallucinations or incorrect decisions which would unfairly prejudice data subjects. Further, allowing individuals to appeal or make representations about any decision made about them using Gen AI will go a long way to assist in mitigating potential biases which may arise when using Gen AI for this purpose. Questions of how the decision was arrived at, what factors assisted in making the decision, and how the algorithm which made the decision was created are all important considerations which businesses must be able to answer, especially should they ever be called to justify why certain decisions were arrived at.

Having a clear policy in place which speaks to these points is key to ensuring privacy compliance. Businesses should have a dedicated policy related to automated decision making to demonstrate that they have considered how automated decision making can impact individuals, how those decisions are made and whether there is the ability to intervene in an outcome.

"The regulatory landscape for Gen AI is defined by the Data Protection Act, 2012 (Act 843) and the Cybersecurity Act, 2020 (Act 1038). Under Act 843, if personal data is being used for model training or fine-tuning, it must be clearly stated. Additionally, developers must have an adequate lawful basis and ensure that any logic behind any automated decision that will significantly impact a data subject must be explainable. To supplement this, the Cybersecurity Act, 2020 requires developers to implement technical safeguards that prevent these models from using personal data to generate malicious synthetic media or deepfakes."

Ghana – Effie Bonful,
Assistant Manager, IT Advisory,
KPMG Ghana

"Automated decision making in Kenya is growing, and many financial institutions are introducing consent clauses in their agreements to address the issues around this. The Central Bank of Kenya is yet to issue guidelines on the use of artificial intelligence, however their recent survey notes that organisations are curious to know about guidance on model transparency and fairness, as well as gaining clarity on managing the use of third-party AI models. It is clear from the Data Protection Act, 2019 that ADM which falls under data processing must be done with consent from data subjects."

Kenya – Raymond Kiyegga,
Manager, Tech Risk,
KPMG Kenya

Bridging policy and practice: a two-step blueprint for Gen AI privacy compliance

Making sure that an organisation's use of Gen AI is lawful and ethical from a privacy perspective requires a two-step approach. The first step involves creating a framework which provides comprehensive, clear and easy to understand guidance on how employees should use Gen AI in their roles.

This framework should consider existing documents which are already part of businesses' privacy programmes, and where there aren't any such policies, create new ones to address any gaps. It involves carefully considering, developing and adopting robust, forward-looking policies within an organisation that foster innovation and safeguard the rights of its data subjects. This framework is not intended to replace any privacy compliance programme, but to work hand in hand with it, and to address other key areas such as the ethical use of Gen AI.

The second part of the approach to ensuring that an organisation meets its privacy goals is training and awareness – a policy is only useful if employees know about it. Businesses should devise an approach that involves a systematic rollout of training to all employees who use Gen AI in their day-to-day roles, and provide them with opportunities to understand how to integrate Gen AI into their functions. As legislation evolves, new employees join the organisation and technology continues to advance, regular reinforcement of training and awareness will play a key role in ensuring that there is consistency in your privacy implementation programme.

What does the future look like for Gen AI regulation?

The future of Gen AI regulation in Africa is poised to evolve rapidly as technology becomes more integrated into business and society. With the increasing adoption of generative AI tools, regulators are expected to strengthen existing frameworks, such as POPIA, or develop new ones, such as the National AI Policy Framework, to address the unique risks and ethical considerations posed by AI. There is likely to be a greater emphasis on transparency, accountability and the responsible use of AI, with new guidelines and standards developed to ensure that AI systems are fair, non-discriminatory and respect individuals' data privacy rights. As global AI regulatory trends emerge, South Africa will need to balance alignment with international best practices and the specific needs of its local context, ensuring that Gen AI is harnessed for positive impact while managing potential data privacy and protection risks.

Farah Jakoet

Senior Legal Manager
KPMG South Africa
T: +27 66 474 2780
E: farah.jakoet@kpmg.co.za

Victoria Pillay

Legal Manager
KPMG South Africa
T: +27 11 647 7111
E: victoria.pillay@kpmg.co.za

Key takeaways

- Have we conducted a data mapping exercise and a data privacy impact assessment at the design and deployment stage to identify and mitigate risks? Have we prepared and published a privacy notice which aligns with the transparency obligations under data privacy?
- Do we have robust mechanisms in place to ensure that any automated decision making is not done solely by Gen AI, and can we explain and justify how such decisions are reached?
- Have we developed a comprehensive framework which addresses the ethical use of Gen AI, which includes an effective training and awareness programme?

Capital Agility

Capital Agility

The multiplier effect in a low-growth era

As South African firms enter 2026, they face a paradox: capital positions, a measure of solvency, are robust, yet opportunities for organic growth remain scarce. Given the high penetration rates of banking and insurance services by global standards and a limited formal employment base, real earnings growth for the average firm is minimal. In this stagnant growth context, idle capital becomes "lazy capital," actively diluting Return on Equity (ROE). As echoed by many financial service firms, "Growth is rare, capital is not."

Profitability in the financial services sector has never been solely about credit risk management, underwriting, or expense efficiencies. Capital Efficiency is a critical factor, represented primarily by the "Capital Multiplier"— the strategy to minimise equity required for each unit of risk without compromising customer safety. As multiple external forces impact the calculations underlying the capital multiplier, risks of substandard returns amplify.

Amidst a shifting geopolitical landscape and growing volatility, South African financial services firms encounter new challenges in capital management. The reliance on traditional compliance-driven capital management approaches is waning. There is an urgent need for novel strategies that are adaptive to regulatory changes, external pressures, and shareholder expectations. In this scenario, Capital Agility emerges as a critical differentiator, distinguishing firms in their quest for improved ROEs.

Capital Agility refers to the strategic ability of banks or insurers to dynamically reallocate, protect, and optimise their capital base in real-time, allowing them to respond effectively to market volatility and low-growth conditions. Unlike traditional capital management, which tends to be periodic and compliance-focused, Capital Agility incorporates an operational mindset that treats capital as a flexible asset rather than a static constraint.

Factors necessitating an agile capital approach:

- **Regulatory expectations**

  In the banking sector, the global prudential reform agenda continues to spur significant reforms locally. South Africa's commitment to aligning with outstanding components of these global reforms—particularly the "Basel III post-crisis reforms"—aims to enhance risk sensitivity and strengthen the resilience of domestic banks. The regulatory reforms, effective July 1, 2025, introduced significant changes in the determination of banks' capital requirements, emphasising Risk Weighted Assets (RWA) within the Capital Adequacy Ratio.

  Following the 2009 financial crisis, reforms such as Basel 2.5, followed by Basel III, reinvigorated the regulatory framework to ensure safety and soundness. Despite some global progress, major jurisdictions such as the United States, United Kingdom, and European Union have yet to implement revised market risk and CVA frameworks. This regulatory lag creates uncertainty and may result in lower capital requirements being held in certain jurisdictions, affecting global comparability. South Africa's proactive implementation of these reforms underscores its dedication to maintaining a robust banking infrastructure, aligning with the G20, and bolstering investor confidence.

  For insurers, while the immediate impact of regulatory changes appears less cumbersome, emerging complexities cannot be ignored. The insurance industry, fortified by risk-based capital foundations through frameworks such as the Solvency Assessment and Management (SAM) framework under the Insurance Act of 2017, faces challenges of updating capital models to accommodate climate risk guidance and increasing operational risks. The transition necessitates demonstrable justifications as regulators pressure firms to adapt from standard models to internal ones reflecting true risk profiles.

- **Economic dynamics**

  The strength of the South African financial sector during the 2020-2022 pandemic period showcased "Involuntary Capital Agility." During this period, regulatory bodies such as the Prudential Authority (PA) and the South African Reserve Bank (SARB) acted swiftly, offering temporary capital relief measures, including allowing firms to draw down capital conservation buffers.

  Private sector agility complements regulatory flexibility. Leading financial groups and major banks not only absorbed the shocks but redesigned their capital structures. They implemented rapid "dividend brakes" to preserve liquidity, utilised strategic reinsurance to handle surging mortality and business interruption risks, and leveraged IFRS guidelines to bolster provisioning buffers. This "wartime" capital management strategy empowered the industry to survive record-high claims and credit impairments, emerging by 2024-2025 with healthier—and sometimes stronger—solvency ratios than before the crisis.

  2026 presents both global and domestic economic challenges for banks and insurers. Whilst there's factors supporting real income tailwinds for households, improved RoE's for banks and insurers will depend on the pace at which interest rates drift down as inflation eases. A firmer Rand typically lowers imported inflation and opens room for SARB interest rate cuts. Lower policy rates generally lift unsecured and mortgage origination with a few quarters' lag. Banks, however, may keep underwriting standards tighter for longer due to non-performing-loans overhang from earlier year vintages. Non-interest-margin revenue could also be compressed. For insurers, competitive repricing can spur churn even as macro fundamentals improve. Lower interest rates also compress investment returns on float/capital for insurers, an area insurers often rely on to boost profit margins.

  In addition, South Africa's economic climate exerts domestic political pressures on banks and insurers. The government expects these firms to make meaningful contributions towards national infrastructure and key investment projects. Balancing political expectations against commercial shareholder value and regulatory financial stability places firms on a challenging tightrope.

- **Geopolitical instability**

  Geopolitical developments have driven deregulation calls in the financial services industry, attributed to low economic growth. Tariff and trade conflicts elevate the risk of regulators enforcing higher capital buffers. Prudential regulators maintain their stance against any dilution of requirements that may compromise financial stability. This is not expected to shift significantly in 2026.

  Geopolitical instability escalates the volatility firms must navigate in capital and liquidity risk management. The continued focus on robust "financial conglomerate" supervisory frameworks and stress-testing for evolving geopolitical risk factors, such as changes in international payment or clearance systems, remains crucially relevant.

  The volatility reality has increased, transforming from pandemic risks to structural catastrophe risks and market fluctuations. Firms lacking agile capital playbooks face sluggishness when the next shock hits or are unable to direct capital toward high-growth digitisation opportunities.

- **Operational challenges**

  Current stress testing capabilities were initially designed for periodic, extensive firm-wide stress scenarios. They lack agility to swiftly run comprehensive scenarios that can support dynamic risk management. Outdated modeling approaches yield counterintuitive results, with excessive reliance on historical data constraining parameterisation and emerging risk assessments.

  Banks face the immediate challenge of updating models and controls to surpass revised RWA rules. Reliance on legacy rules-calibrated internal models requires comprehensive updates for alignment with new regulatory definitions. Remediating data pipelines and enhancing governance are vital for credible RWA quantification.

  Regulatory guidance often remains complex or ambiguous, engendering interpretational differences. This may result in inconsistencies in RWA computation within the banking sector.

The Capital verdict: leading in ROE

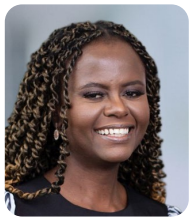
In 2026, financial groups with the most mobile, not necessarily the largest capital buffers, will excel in the ROE race. South African firms showed agility in survival—now they must exhibit agility for growth. Low-growth environments demand Return on Equity (ROE) beyond traditional premium growth, non-interest margin revenue or expense efficiencies. Capital Agility enables ROE "manufacturing" by reducing idle capital, leveraging alternative risk transfer mechanisms for risk alignment, and strategically deploying early-warning indicators.

Capital Agility is a strategic imperative. It ensures real-time capital reallocation, protection, and optimization, essential for firms to maintain competitiveness. As 2026 unfolds, codifying these playbooks ensures firms hold "dry powder" ready, while competitors may stall in deliberations. Capital agility has transcended being a luxury—it's crucial for succeeding in a low-growth era.

Building robust capital agility capabilities will empower firms to dynamically navigate an uncertain future, improving their resilience and capacity for leveraging growth opportunities.

Marius Botha

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



Sebenzile Mathebula

Partner
Financial Services
KPMG South Africa
T: +27 67 599 6833
E: sebenzile.mathebula@kpmg.co.za

Key takeaways

- **Fast-Cycle ICAAP/ORSA and Tactical Triggers:**
  Regulatory capital requirements are static calculations, whereas the Own Risk and Solvency Assessment (ORSA) for insurers and Internal Capital Adequacy Assessment Process (ICAAP) for banks are forward-looking strategic tools, assessing risks' long-term impact on firms' balance sheets and solvency. Implement more frequent "mini-ORSA/ICAAPs", especially when there are significant changes in risk profile, business strategy, or market conditions, with trigger rules for rapid evaluation of capital multipliers within cycles, aligning risk appetites and capital strategies to higher projected capital needs.
- **Disciplined Scenario Setting and Stress Testing:**
  As risk landscapes evolve, banks and insurers should refine stress-testing scenarios to increase strategic accuracy. Comprehensive scenario adjustments will update and refine capital buffers, ensuring effective management even during unexpected disruptions.
- **Enhanced Group-Wide Capital Mobility:**
  Conduct fungibility audits annually to identify "trapped capital" at subsidiaries. Prioritise capital optimisation, including a revaluation of bank arrangements that may be capital intensive. Reassess intra-group reinsurance arrangements, employing internal vehicles for risk centralisation and diversification benefits. Explore alternatives like Lloyds' co-insurance or external securitisations, boosting capital flows for conglomerates.
- **Independent Model Validation and Capital Unlock:**
  Tighten model validation to unlock capital buffers held due to uncertainty. Transition from Standard Formula to Internal Models, contingent on rigorous model validation satisfying Prudential Authority standards, potentially releasing significant Tier 1 capital.
- **AI Integration in Capital Management:**
  Embrace AI for complex capital management integration. AI-driven models surpass traditional analyses, enabling scenario simulations and dynamic reserving, releasing previously held reserves to optimise capital deployment.

Cyber Security

Cyber Security

From compliance burden to growth enabler

Over the past 10–15 years, the evolution of cybersecurity regulations in Africa has meaningfully changed how businesses operate, especially as economies have digitised.

The evolution of cybersecurity regulation in Africa is closely tied to the continent's digital transformation journey – from scattered responses to coordinated frameworks intended to:

- Protect citizens and business online
- Enable secure digital economies
- Enhance cross border cooperation
- Safeguard digital rights alongside security.

Key notes for infographic:

- Cybersecurity regulation in Africa has moved from fragmentation to structure
- Regulatory maturity closely follows digital economic activity
- Enforcement — not law-making — is the key differentiator
- Businesses must tailor compliance strategies by region.

Evolution of cybersecurity regulations in Africa

Phase 1 — Foundations & Early Signals (Early 2000s)

What it looked like
- ICT, telecoms, and interception laws
- No dedicated cybersecurity focus
- Cyber issues handled under general criminal law.

Key characteristics
- Fragmented regulation
- Weak enforcement
- Low awareness of cyber risk.

Phase 2 — National Cybercrime Laws Emerge (2010-2014)

What changed
- First standalone cybercrime and data protection laws
- Recognition of online fraud, hacking, and digital evidence.

Key developments
- Ghana Data Protection Act (2012)
- South Africa POP1A (2013)
- Early national cybersecurity strategies.

Impact
- Legal recognition of cyber threats
- Focus on crime and enforcement rather than resilience.

Phase 3 — Continental Vision & Fragmentation (2014-2020)

Milestone

2014: AU Malabo Convention adopted

Reality
- Strong continental framework
- Slow ratification and uneven implementation
- Countries continue developing national laws independently.

Trends
- Cybercrime laws expand
- Data protection authorities established
- CERTs begin to appear.

Phase 4 — Enforcement, Reporting & Accountability (2020- 2023)

Major shift
- Regulations move from paper laws to operational enforcement.

New features
- Mandatory breach reporting
- Executive accountability
- Sector-specific cybersecurity rules
- POPIA and Cybercrimes Act enforcement (SA)
- Financial-sector cyber regulations expand.

2023 milestone
- Malabo Convention enters into force.

Phase 5 — Digital Economy & Resilience Focus (2024-Present)

Current direction

Cybersecurity embedded in:
- Digital transformation strategies
- Data governance frameworks
- Critical infrastructure protection
- AI and emerging technology policy.

Key themes
- Resilience over prevention
- Cross-border cooperation
- Alignment with global standards
- Cybersecurity as economic infrastructure.

How has the evolution of cybersecurity regulations in Africa impacted businesses operations?

As African economies digitise at speed, the evolution of cybersecurity regulation has become a critical enabler of digital transformation and sustainable economic growth.

Cybersecurity shifted from "IT issue" to "strategic business risk"

One of the most significant impacts of regulatory evolution has been the elevation of cybersecurity from a technical concern to a board-level issue. Modern laws (cybercrime acts, data protection laws, critical infrastructure rules) place legal responsibility on organisations, and in some cases accountability on directors or executives. The business impact is that Boards now discuss cyber risk alongside finance and legal risk, Cybersecurity policies, audits, and reporting structures have become standard and enterprise risk management frameworks increasingly include cyber threats. Cyber resilience is now directly linked to operational continuity, reputation, and valuation.

Digital growth needed trust before it could scale

Africa's early digital successes — mobile money, digital platforms, and online services — emerged faster than the legal and institutional frameworks needed to secure them. While innovation flourished, trust lagged. High fraud levels, inconsistent standards, and weak accountability limited how far digital solutions could scale. Consumers hesitated, investors priced in risk, and businesses absorbed losses quietly.

Cybersecurity and data protection regulations changed this dynamic. By establishing clear rules for data handling, breach reporting, and cybercrime, governments created the trust infrastructure necessary for digital systems to move from pilot projects to national and regional platforms. Regulation transformed digital tools into reliable economic infrastructure.

Compliance costs and operational restructuring increased

As regulations matured, businesses had to change internal operations to stay compliant which include hiring or outsourcing cybersecurity and compliance specialists, creating roles such as Data Protection Officers (DPOs), implementing internal controls, access management, and audit trails, as well as investing in secure infrastructure, encryption, and monitoring tools. This had a financial impact due to higher operating costs, especially for SMEs and Compliance budgeting, which became a recurring business expense.

Mandatory breach reporting changed incident handling

In the past, many cyber incidents were quietly handled, or ignored. With newer regulations businesses must report breaches to regulators within defined timelines and notify affected customers. Failure to disclose can attract fines and reputational damage. Cyber incidents now trigger legal and reputational consequences, not just downtime.

Data handling and customer trust practices evolved

The rise of data protection and cybersecurity laws forced companies to rethink how they collect, store, and use data. This resulted in changes in data minimisation and retention policies, consent management and privacy notices, stronger controls over third-party vendors and cloud providers and cross-border data transfer assessments. The resulting effect being more transparency with customers, improved trust in fintech, telecoms, and e-commerce, as well as alignment with global partners that require strong data protection standards.

Sector-specific operations became more regulated

Certain sectors experienced the impact more strongly:

- Financial services: stronger security standards, transaction monitoring, reporting duties
- Telecoms: infrastructure protection, lawful interception obligations
- Energy & utilities: critical infrastructure protection requirements
- Fintech & startups: licensing increasingly tied to cybersecurity maturity.

This resulted in security requirements becoming part of licensing and market entry and businesses having to embrace the concept of "security by design" with security "built in" and not added later.

Cross-border business became more complex — but clearer

As countries introduced national laws (often inspired by regional or global frameworks) businesses operating in multiple African countries had to navigate different legal requirements. Legal and Compliance teams became more involved in expansion plans, contracts now include cybersecurity and data-protection clauses, and due diligence on partners and vendors intensified.

Increased investor and partner scrutiny

Cybersecurity regulation changed how businesses are evaluated by investors, banks, international partners, and regulators. Today weak cybersecurity can block funding or partnerships, compliance improves credibility and valuation, and Cyber maturity is increasingly seen as a sign of operational stability

Skills shortages affected day-to-day operations

Regulation increased demand for cybersecurity skills faster than supply resulting in competition for skilled professionals, reliance on managed security service providers, and training and upskilling became necessary operational strategies.

Overall impact

Across Africa, cybersecurity regulations have had a multipronged impact — driving transparency, elevating accountability, criminalising cyber threats, encouraging harmonisation, and nudging organisations toward better risk management. While enforcement and capacity remain uneven, the overall trajectory reflects a shift from reactive measures toward strategic, legal, and institutional frameworks that support digital trust and secure economic growth.

Cybersecurity regulatory evolution to digital transformation and economic growth

For much of Africa's digital journey, cybersecurity regulation was viewed primarily as a constraint — a cost of doing business in an increasingly connected economy. Today, that view is outdated. At some point cybersecurity regulation stopped being a "cost story" and becomes a growth story. The evolution of cybersecurity regulations in Africa has been tightly intertwined with digital transformation and, by extension, economic growth. The thinking is that of regulation as the trust infrastructure that allowed digital economies to scale.

Key outcomes of cybersecurity regulations:

- **Unlocked participation in the formal economy and supported financial inclusion and SME digitisation**. Secure digital systems bring more people and businesses into the formal economy. Cybersecurity regulation directly supports digital trust, which is essential for economic inclusion

- **Accelerated fintech, e-commerce, and platform economies.** Africa's fastest-growing digital sectors — fintech, telecoms, e-commerce, and platform services — rely heavily on secure systems. Regulation didn't slow innovation — it made scaling possible

- **Led to an increase in foreign investment and global integration.** Global investors and partners care deeply about data protection, cyber risk and regulatory certainty. As African countries adopted clearer cybersecurity frameworks investor confidence improved and African firms could tap into global value chains. This resulted in growth in tech-enabled exports, expansion of digital services trade, and stronger integration into the global digital economy. Cyber regulation acted as a signal of market maturity

- **Shaped more sustainable innovation**. As laws matured, businesses were forced to design security into products ("secure by design"), build resilient digital systems and invest in skills and infrastructure. This resulted in more resilient digital ecosystems, lower systemic risk and sustainable innovation rather than short-lived hype. Cyber regulation supports quality growth, not just rapid growth

- **Resulted in economic trade-off: short-term cost, long-term gain** There is a trade-off in that compliance increases costs in the short term but over time costs fall as standards mature, shared infrastructure emerges, and trust-driven adoption accelerates growth. The net effect is higher long-term economic returns from digital transformation.

What does this mean for business leaders?

As African economies digitise at speed, the evolution of cybersecurity regulation has become a critical enabler of digital transformation and sustainable economic growth. For business leaders, understanding this shift is no longer optional; it is central to competitiveness, investment readiness, and long-term resilience.

Cybersecurity regulation in Africa has evolved from a defensive necessity into a foundation that allowed Africa's digital transformation to become an engine of economic growth, not just technological change. Executives who treat it purely as a compliance exercise risk falling behind. Those who integrate cybersecurity into strategy, product design, governance, and expansion planning will be better positioned to thrive in Africa's rapidly digitising economy.

In today's Africa, digital growth follows trust — and trust is increasingly regulated.

Judith Masekwameng

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

Key takeaways

- To keep ahead of the evolving cybersecurity regulations, organisations should strengthen cyber governance and treat cybersecurity as a strategic risk discipline.
- Build a control-based compliance model where controls are mapped to multiple regulatory frameworks.
- Invest in continuous monitoring so you have real-time oversight to enable your organisations to be proactive.
- Run regular resilience testing for critical business operations. Resiliency is key to adapt and delivery critical services without losing stakeholder trust.

Artificial Intelligence

Artificial Intelligence

Regulatory reframing of AI risk - from use to outcomes

Regulators have shifted focus from questioning *whether* organisations use AI to evaluating how AI systems perform in terms of transparency, fairness, accountability, and governance. This shift acknowledges that AI related decisions are no longer peripheral technical issues, but executive and risk management concerns affecting trust, consumer outcomes, systemic resilience, and market integrity.

Emerging risk areas include:

- **Consumer protection and fairness:** Automated decisions in credit scoring, pricing, and claims handling carry risks of bias and discrimination
- **Data protection and privacy:** AI systems require vast datasets for training and decisioning, making personal data governance central to regulatory oversight
- **Operational resilience:** The complexity of AI systems introduces novel failure modes and dependencies on data quality and third-party service providers.

These risk categories require regulators to treat AI as part of the regulated control environment, even where standalone AI laws are not yet in force.

In Africa, with varying degrees of regulatory maturity, treating AI as a regulated decision capability rather than a technological novelty has become a competitive and compliance imperative. AI is reshaping the regulatory landscape for financial services in South Africa and across Africa, incorporating insights from key regulatory thinking and industry perspectives.

Third party and embedded AI: the accountability gap

A significant regulatory challenge arises from the increasing use of embedded AI, that is, AI capabilities embedded within third-party platforms such as core banking systems, customer relationship management (CRM) tools, fraud engines, or cloud services.

Regulators increasingly emphasise that accountability for AI outcomes cannot be outsourced, even where the technology is procured from third parties. This regulatory stance mirrors broader trends in outsourcing and operational resilience guidance where financial institutions remain fully accountable for outsourced processes and must demonstrate effective governance regardless of whether the technology originates internally or from third parties.

In South Africa, outsourcing and third-party risk management guidelines issued by the Prudential Authority and Financial Sector Conduct Authority (FSCA) apply equally to systems incorporating AI — meaning institutions must ensure oversight, auditability, and assurance even where AI logic is opaque or proprietary to vendors.

Data protection laws and AI governance convergence

In Africa, explicit AI laws remain largely absent. Instead, data protection statutes act as the de facto regulatory framework shaping AI governance. The regulatory approaches in countries across the continent illustrate how existing frameworks are being applied to AI:

- **Nigeria** has outlined an AI strategy and is progressing legislative efforts (e.g., National Digital Economy and E-Governance Bill) to expand supervisory powers over AI systems. Nigeria's Data Protection Act 2023 establishes key legal requirements for personal data use, especially regarding profiling and automated decision-making
- **Ghana** takes a more principles-led approach, relying on data protection and cybersecurity legislation and collaborative sector regulation. Ghana's Data Protection Act 2012 (Act 843) provides similar foundational safeguards.

These statutes implicitly govern AI-related activities by controlling how data, including personal data, can be collected, used, shared, and stored. Failure to align AI systems with data protection requirements can lead to regulatory enforcement actions even in the absence of AI-specific laws. This linkage between data governance and AI governance underscores the need for strong data discipline in any AI implementation.

In both countries, AI regulation is not yet mature, but the emphasis on existing laws suggests a transitional period where supervisors enforce outcomes rather than technological form. By 2026, Nigeria and Ghana share a common regulatory reality. The most enforceable controls on AI do not sit in stand-alone AI laws but within existing data protection and cybersecurity regimes. The real risk is not AI in theory, but AI embedded in high-impact financial decisions where governance, accountability, and oversight are weak.

Regional coordination through ECOWAS to modernise data protection frameworks and integrate AI considerations is steadily improving alignment and cross-border consistency. This is creating a shared baseline for supervisory expectations across West Africa.

Divergence is likely to emerge in pace and form. Nigeria appears set to move faster toward baseline AI standards through national AI strategy instruments, a potential AI code of practice, and a digital governance bill that would make supervisory intervention more explicit. Ghana's approach remains more principles-led, relying on existing data and cybersecurity legislation, with AI oversight expected to mature through sector regulators rather than new horizontal rules.

- **South Africa**

South Africa's regulatory architecture is characterised by sectoral oversight applications of existing laws rather than horizontal AI legislation. For example:

- **South Africa's Protection of Personal Information Act (POPIA)** governs the lawful processing of personal data and includes protections against decisions based solely on automated processing. Please see our article on Data Privacy in this publication for more information
- **FSCA's conduct and consumer protection mandates** extend to automated decision-making
- **Prudential supervision** emphasises operational resilience and risk governance
- **Cybersecurity frameworks** address the intersection of AI, data security, and continuity planning.

This layered regulatory posture aligns with the UK's principles-based model of AI oversight, which prioritises outcomes, transparency, and accountability over prescriptive obligations.

Industry perspectives: AI investment vs regulatory progress

The KPMG 2025 Banking and Capital Markets CEO Outlook reveals that bank CEOs are increasingly prioritising AI investment, with significant expectations for return on investment within the next one to three years.

These insights underline a tension between rapid AI adoption and the need for robust governance. Notably, CEOs recognise that ethical concerns and governance gaps are among the major challenges — with regulatory uncertainty cited as a barrier to AI deployment. Furthermore, the acceleration of AI budgets reflects confidence in near-term value while acknowledging that responsible deployment is essential to unlock that value. In KPMG's broader Africa CEO Outlook, many CEOs identify AI integration as a strategic priority — ranking alongside regulatory pressures and cybersecurity risks.

These industry views reinforce a central regulatory concern: financial institutions must balance AI innovation with governance capability, including risk management, data discipline, and regulatory compliance.

Governance, King V and emerging technologies

Although South Africa does not yet have a dedicated AI statute, the principles of the King IV Report on Corporate Governance (King IV) are directly applicable to AI-enabled decision-making.

King IV emphasizes ethical leadership, responsible corporate citizenship, effective risk governance, technology and information governance, and transparent stakeholder communication. AI systems deployed in financial services directly implicate these principles. Algorithmic credit decisions, automated pricing models, fraud detection systems, and generative AI tools are not merely operational tools — they are governance matters that affect fairness, accountability, and stakeholder trust.

In particular Principle 12 (Technology and Information Governance) requires governing bodies to oversee technology in a way that supports strategic objectives while managing risk. AI model deployment therefore becomes a board-level responsibility rather than a purely technical function. Boards must ensure AI risks are identified, assessed, monitored, and disclosed appropriately.

As emerging technologies accelerate, institutions that align AI governance with King IV principles will be better positioned to demonstrate ethical conduct, resilience, and regulatory readiness.

Key constraints in AI regulation

Despite momentum, several constraints hamper effective AI regulation in financial services across the continent:

- **Informal, decentralised adoption:** Business units often deploy AI before governance frameworks mature or have adapted their controls
- **Limited model transparency:** Embedded and vendor-owned AI models present challenges for explainability and regulatory scrutiny
- **Data quality issues:** Biased, incomplete, or non-representative data amplifies unfair outcomes, making data discipline a foundational requirement for effective AI assurance
- **Fragmented oversight:** Overlapping supervisory mandates (data protection, cybersecurity, financial conduct, prudential supervision) complicate coherent governance. slowing the development of coherent AI supervision frameworks
- **Capability gaps:** Regulators require specialised skills and tooling to audit and evaluate complex AI systems.

These constraints are observed across African and global jurisdictions and are widely acknowledged in industry research. The KPMG CEO outlook reports highlight that regulatory uncertainty, data readiness, and ethical issues are prominent CEO concerns related to AI implementation — further underscoring the intersection of governance and risk.

Trusted and Responsible AI as a Strategic Imperative

As AI adoption accelerates, regulatory focus is converging on the concept of Trusted and Responsible AI — a framework that integrates governance, ethics, transparency, and accountability into AI design and deployment.

Drawing on leading practices, including global industry frameworks, responsible AI rests on core pillars including fairness and bias mitigation, transparency and explainability, accountability and clear ownership, data integrity and privacy protection, security and resilience, and human oversight and redress mechanisms

For financial institutions, trusted AI is not merely a compliance requirement — it is a strategic enabler. Institutions that embed responsible AI principles reduce regulatory exposure, strengthen board oversight, enhance consumer trust, improve model reliability, and enable sustainable AI scaling

Importantly, regulators increasingly expect institutions to evidence governance over AI outcomes — not simply technical performance. This requires formalised model inventories, risk classification frameworks, outcome monitoring, and documented oversight structures.

Financial institutions that adopt a Trusted AI governance model aligned to King IV principles and emerging regulatory expectations will be better positioned to demonstrate both innovation capability and regulatory maturity.

Forward looking actions

While explicit AI regulations are still being articulated, organisations need to act ahead by focusing on the identified AI risk areas. Financial services firms should classify AI by regulatory impact, clearly distinguishing productivity tools from high-impact decision engines that directly affect customers and markets. AI should be embedded into enterprise risk governance, treated as part of the regulated control environment rather than a standalone technology initiative, and aligned with data protection, cybersecurity, and conduct obligations. It is critical that outcomes are measured, not just model performance. Fairness, explainability, and redress indicators should sit alongside accuracy metrics in risk reporting.

Third-party governance should be strengthened by updating procurement and vendor risk frameworks to require model documentation, change logs, security attestations, and audit rights for embedded AI. Firms should also prepare for regional convergence, tracking developments and designing cross-border controls for data transfers, model portability, and incident sharing at scale.

A defining regulatory challenge

AI is a defining regulatory challenge for the financial services sector in Africa. While legislative frameworks specifically addressing AI are still under development, regulators are growing more assertive in applying existing legal constructs and supervisory tools to govern AI-enabled decisioning.

Industry sentiment highlights both the acceleration of AI adoption and the emergence of ethical, data, and regulatory concerns. These dual pressures — strategic innovation and governance reliability — reflect a broader truth: AI's regulatory challenge is not just about compliance, but about trust, fairness, and resilience in a rapidly evolving financial ecosystem.

Organisations that proactively treat AI as a regulated decision capability - governed with the same discipline as credit, conduct, and operational risk - will be better positioned to scale innovation, maintain regulator confidence, and protect trust in an increasingly automated economy.

Pranesh Kara

Partner
Technology Risk
KPMG South Africa
T: +27 82 719 1402
E: pranesh.kara@kpmg.co.za

Ladi Asuni

Partner
Technology Platforms
KPMG Nigeria
T: +23 480 397 54101
E: ladi.asuni@kpmg.co.za

Key takeaways

- **Clear accountability:** Boards and senior management must own AI risk decisions. Regulators will expect named ownership of AI-related risk at board and senior management levels, supported by documented approval processes and ongoing oversight.
- **Fairness and non-discrimination:** Regulators will expect named ownership of AI-related risk at board and senior management levels, supported by documented approval processes and ongoing oversight.
- **Explainability and transparency:** Firms will need to explain AI decisions to both customers and supervisors in clear, plain language and to reconstruct model logic and data lineage when challenged by regulators.

Cross Border Payments

Cross Border Payments

The structural complexity of Africa's cross-border payments

The core question

Despite years of reform, technological innovation and regulatory focus, cross-border payments in Africa remain slow, costly and operationally complex. This is not simply a technology problem, nor is it purely a regulatory one. The complexity of cross-border payments is structural, rooted in the way Africa's financial systems, currencies, regulations and institutions have evolved independently. Understanding why cross-border payments are so cumbersome is essential for executives seeking to scale regionally, support intra-Africa trade, and manage regulatory risk.

Cross-border payments connect multiple sovereign systems, not one market

Unlike domestic payments, cross-border transactions span multiple sovereign monetary, legal and regulatory systems. Each payment must comply simultaneously with:

- The rules of the sending country,
- The rules of the receiving country, and
- Often the rules of one or more intermediary jurisdictions.

In Africa, this complexity is intensified by the fact that each country operates its own currency, and has its own central bank, foreign exchange (FX) regime, and regulatory framework. Even where regional economic communities exist, regulatory authority remains largely nationalised. This means that a single cross-border payment is, in effect, a chain of domestic payments stitched together, each with its own compliance requirements.

Currency and foreign exchange controls are deeply embedded

Foreign exchange regulation is one of the most significant, and least visible, sources of friction in cross-border payments.

Many African economies use FX controls to protect monetary stability, manage scarce hard currency reserves, and mitigate capital flight.

While these objectives are legitimate, they introduce complexity and resultant time lags into payment flows. Cross-border payments often require currency conversion, regulatory approval, and / or offshore settlement. As a result, payments that appear simple from a customer perspective can involve multiple FX legs and settlement pathways behind the scenes.

Initiatives such as the Pan-African Payment and Settlement System (PAPSS), supported by Afreximbank, aim to reduce this dependency by enabling local currency settlement, but adoption and scale remain a challenge.

Compliance obligations multiply across borders

Cross-border payments sit at the intersection of payments regulation, financial crime controls, sanctions compliance, and consumer protection requirements.

Regulators across Africa for example, apply FATF-aligned AML/CFT[1] standards, but implementation and supervisory interpretation vary significantly. As a result, institutions must apply multiple risk frameworks to a single transaction, often defaulting to conservative controls to avoid regulatory breaches.

[1] FATF – Financial Action Task Force; AML – Anti-Money Laundering; CFT – Counter-Terrorist Financing

For banks and payment service providers, this means:

- Duplicated checks being executed across jurisdictions
- Higher transaction rejection rates; and
- Ultimately, increased operational cost.

The faster the payment needs to be completed, the harder this compliance balancing act becomes, a challenge which is heightened as more African markets move towards growing real-time domestic payments.

Payment infrastructure has evolved domestically, not regionally

Across Africa, significant investment has been made in domestic payment system modernisation, including real-time payment rails and increased digital access. In Southern Africa, for example, the South African Reserve Bank's Payments Ecosystem Modernisation (PEM) programme prioritises domestic payments modernisation through interoperability and standards adoption, supported by infrastructure modernisation, increasing platformisation of payment services, and an evolving governance model for the payments ecosystem.

However, cross-border connectivity has lagged. Legacy domestic systems were not originally designed to operate across borders, currencies and regulatory regimes; and resultantly are not always as scalable as needed. As a result, cross-border payments often rely on correspondent banking networks, offshore settlement currencies, and manual reconciliation processes.

This structural mismatch means that payments are only as fast and efficient as the weakest link in the chain.

Regional harmonisation exists, but only within limits

Some regions have made meaningful progress. In West Africa, the Central Bank of West African States (BCEAO) provides harmonised oversight of payment systems within the West African Economic and Monetary Union (WAEMU) region, reducing friction for intra-zone transactions. Similarly, the East African Community (EAC) promotes financial sector integration and interoperability.

However, even in these regions, harmonisation does not eliminate differentiated FX controls, differing supervisory expectations, or national enforcement priorities. As a result, regional integration improves efficiency but does not remove the fundamental complexity of cross-border payments.

Regulation is both a source of complexity, and the solution

Regulation contributes to cross-border payment complexity by reflecting national policy priorities around (amongst others) financial stability, financial crime and consumer protection. At the same time, regulation is also the primary mechanism through which complexity can be reduced.

Global frameworks, such as the G20 Roadmap for Enhancing Cross-Border Payments, articulate clear objectives around cost, speed, transparency and access. At a continental level, the AfCFTA[2] Protocol on Trade in Services recognises the importance of efficient payments for economic integration.

The challenge is not a lack of regulatory intent, but the coordination and execution of reforms across multiple jurisdictions.

[2] AfCFTA – African Continental Free Trade Area

Why this matters for the C-suite

For executives, cross-border payments complexity manifests as:

- Higher costs and lower margins
- Slower time-to-market for regional offerings
- Increased compliance and operational risk; and
- Inconsistent customer experiences.

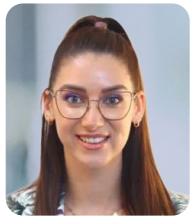
Importantly, this complexity is structural and persistent. It cannot be "fixed" by technology alone.

Shaping the regulatory landscape for harmonised payments

Regulators must actively shape the future of cross-border financial services. Based on global principles from bodies such as the BIS CPMI[3], IMF[4], World Bank, and Africa specific initiatives like PAPSS and AfCFTA, the key considerations for regulators include:

- Collaborating towards fundamental regulatory harmonisation across jurisdictions, on key topics such as KYC5 / AML / CFT, licensing regimes, FX rules, and common dispute resolution and consumer protection frameworks (which will also further enable regional data-sharing to strengthen AML / CFT and transaction monitoring)
- Promoting interoperability between countries, payments schemes, and stakeholders, for example leveraging recognised standards such as ISO 20022
- Supporting and aligning enabling payment infrastructure, including instant payment systems (e.g. PAPSS), shared mobile money platforms, regional FX platforms, and digital identity systems
- Establishing governance and regional cooperation as a collective mechanism to drive alignment (e.g. regional payment councils or leveraging existing collaborative working groups across central banks and supporting regulators).

Cross-border payments in Africa will become simpler, but not imminently, and not uniformly. Progress will likely be incremental and enabled by regulatory coordination, infrastructure interoperability, and market adoption. Institutions which succeed will be those that understand the underlying sources of complexity, engage regulators proactively and design payment strategies that accommodate, rather than fight, regulatory and structural realities.



Daniella de Gouveia

Senior Manager
Digital & Customer Advisory Payments & Financial Services
KPMG South Africa
T: +27 66 307 0846
E: daniella.degouveia@kpmg.co.za

[3] BIS CPMI – Bank for International Settlements Committee on Payments and Market Infrastructures

[4] IMF – International Monetary Fund

[5] KYC – Know Your Customer

Key takeaways

While regulatory frameworks evolve, FS institutions must not wait. Instead, they should act now to ensure shorter-term sustainability and effectiveness by:

- Designing cross-border payment strategies around structural complexity, not best-case assumptions.
- Proactively collaborating with regulators on emerging cross-border use cases, particularly those involving FX and financial crime controls, by leveraging regulatory sandboxes to co-create safe, scalable innovation.
- Investing in interoperable infrastructure and regional partnerships that can scale as harmonisation progresses.

Lean Regulatory Risk Management

Lean Regulatory Risk Management

High-impact, demonstrable outcomes that protect capital and consumers.

Balancing regulatory friction versus operational viability

As South African insurers and banks navigate stagnant real-GDP growth in 2026, the traditional "add-on" model of compliance has reached its fiscal limit. Emerging risk management and compliance with more regulations have become too expensive for many financial services firms. The cost of regulatory friction is a direct threat to operational viability and Return on Equity (ROE).

The temptation with growing compliance costs is to continue cost-cutting initiatives in control function budgets and resources. This, however, may not be a smart move. Rather, applying lean principles to compliance and risk management may provide better outcomes. The South African financial services industry, like its global peers, is moving towards Lean Regulatory Risk Management. This is a paradigm shift that replaces "tick-box" compliance with a surgical, risk-based approach.

The objective is no longer to be 100% compliant with every regulatory sub-clause simultaneously, but to achieve scalable and efficient compliance- and risk management that directs resources precisely where impact tolerances are at risk. "Lean regulatory risk management" aims to maximise value and minimise waste—in the specific domain of identifying, assessing, and mitigating risks associated with laws, regulations, and supervisory expectations – without losing independent judgement from first line management.

The outcome is an efficient, integrated, and continuous process that avoids unnecessary bureaucracy and supports agile decision-making while ensuring compliance.

How is this achieved?

From "everything" to "impact" (risk-based prioritisation)

The primary failure of legacy compliance is the equal weighting of all controls and limited resources. In 2026, lean-minded Chief Risk Officers (CRO's) are adopting a "zero-based compliance" mindset:

- Instead of broad monitoring, focus available budget and investment where impact tolerances for critical business services are most at risk of breach. If a control does not directly protect a conduct outcome or prevent a material systemic failure, it is a candidate for de-scoping. Don't just de-prioritise; cut monitoring and reporting on low-risk compliance areas.
- In a low-growth cycle, firms must aggressively de-scope "nice-to-have" controls that provide marginal risk reduction but high operational friction. This is not about cutting corners, but about cost-effective compliance that satisfies regulators' expectations through quality over quantity.
- Investments should be funnelled into proving demonstrable compliance in high-priority areas such as cybersecurity and conduct outcomes, rather than maintaining static plans, registers, and documentation.

The "local adapter" model (scalable compliance)

For South African groups operating across heterogeneous jurisdictions in the rest of Africa, the cost of duplicative compliance functions is unsustainable.

- Lean firms are building scalable group frameworks based on a single core policy (e.g., a global Anti-Money Laundering or Data Privacy standard) supplemented by local adapters—specific annexes that address unique jurisdictional requirements like the CIMA Code in West Africa or risk-based capital regimes in East Africa
- Industrialise controls at the core where they matter most—eg. product governance, claims outcomes, and cyber resilience. By standardising these "core" controls at the group level, firms can achieve economies of scale while remaining agile enough to meet the Financial Sector Conduct Authority (FSCA)'s specific demands in the South African market. Review processes should be systematic, automated, and scalable, rather than relying on manual, fragmented, or ad-hoc approaches.

Automate the standard risk management lifecycle

To transition from manual compliance-and risk management friction to industrial scale efficiency, CROs should direct teams on a clear incremental automation path. The transformation can be operationalised through the following:

Phase 1: Assessment & Strategy (Q1 2026)

- Reflect on and debate the risk gap analysis. Identify redundancies and inefficiencies in existing reporting frameworks
- Ensure controls mapping is visible to all stakeholders. Use automated templates and dashboards to link requirements (e.g., ISO 27001, COFI conduct risk controls) to existing proof of implementation.

Phase 2: Building Core Elements (Q2 2026)

- Unify risk- and compliance data into a single repository to ensure a "single source of truth" for reporting. Invest in central register consolidations
- Assign policies to employees based on roles and automate tracking of sign-offs. Automate the policy management process.

Phase 3: Continuous Monitoring & Testing (Q3 2026)

- Evolve dashboards for real-time oversight of compliance status and exception tracking
- Pull live data from cloud services and identity systems so compliance status reflects reality, not just paperwork. Automate evidence collection as far as possible. Use forums for qualitative enhancements and risk thinking.

Phase 4: Review & Refinement (Q4 2026)

- Use AI agents to triage incidents, predict risks, and analyse (e.g. transaction metadata for AML). Let AI provide the baseline insights
- Conduct lessons-learned sessions to refine the roadmap for the following year. Be deliberate in conducting an annual review that aims to refine and make your risk organisation even more lean next year

Be cost disciplined

The key to lean compliance is knowing where to be "heavy" and where to be "light."

- Automate and standardise areas such as AML/KYC and product oversight. These are high-volume, high-scrutiny areas where technology can significantly lower the unit cost of compliance. However, beware of poor return-on-investment decisions. Not all risk- and compliance platform trends will deliver sustainable value to your firm
- For internal administrative regulations and low-risk operational areas, move toward self-certification and exception-based reporting. This releases the compliance team to act as strategic advisors rather than clerical checkers. Simplify all low impact areas.

Anticipate where the firm's strategic evolution will hit the regulatory horizon

To maintain a lean posture, CROs must anticipate the strategic direction of travel. Prioritise the risk touch points that could set the organisation's back strategically. You can drop rubber balls that can bounce back, but don't drop glass balls.

Major examples for 2026 are:

Framework	2026 Regulatory Issue	Risk Created	Lean Strategy
COFI Bill	Shift to **activity-based** licensing and outcomes-focused conduct.	Significant restructuring costs if handled reactively.	**Map activities early**; embed a customer-centric culture rather than building massive new reporting layers.
Cyber Resilience	Joint Standard on Cybersecurity requiring **demonstrable resilience**.	Heavy IT investment requirements in a high-threat environment.	Focus on **cyber hygiene** and material incident reporting rather than exhaustive audits of low-risk systems.
ISSB & ESG	Mandatory sustain-ability reporting and **climate-related risk** disclosures.	"Greenwashing" risk and high data aggregation costs.	Integrate ESG into existing **ERM frame-works** rather than creating a standalone silo.
POPIA	Mature enforcement era; high focus on **third-party risk**.	Reputational damage and heavy fines for data breaches.	Simplify third-party management through **automated screening** of high-risk vendors only.

Have honest conversations with management on regulatory impact

To help firms distinguish between critical and non-essential controls, utilise a Regulatory Impact Assessment (RIA) Matrix. This matrix evaluates regulations based on their potential to cause systemic failure or harm consumer outcomes. Involve first-line experts in the assessment.

Regulatory Impact Assessment (RIA) Matrix

The following Regulatory Impact Assessment Matrix shows where to focus for maximum regulatory and operational impact:

Priority Level	Criteria	Example (2026)	Lean Action
Critical	Direct impact on solvency or "Treating Customers Fairly" (TCF) outcomes.	Risk Weighted Assets (RWA) under Banking Capital Adequacy Requirements; COFI conduct standards.	**Industrialise:** Automate controls and invest in real-time monitoring.
Essential	Required for legal license to operate but lower immediate risk to customers.	AML/KYC; Beneficial Ownership verification.	**Standardise:** Use group-wide policies with "local adapters" for efficiency.
Operational	Procedural requirements with lower impact on financial stability.	Routine administrative returns; CPD tracking (where reduced).	**Simplify:** Move to ex-ception-based reporting or self-certification.
Nice-to-Have	Internal "gold-plating" beyond regulatory necessity.	Excessively frequent internal audits of low-risk departments.	**De-scope:** Remove or reduce frequency to focus on high-impact areas.

Survey to identify "regulatory waste"

To execute a lean compliance-and risk management strategy, continuously elicit views from the board, management and key first-line managers whether any of the Seven Deadly Wastes are present:

Waste Type	Definition in a Regulatory Context	2026 Example	Key Questions and Lean Actions
Overproduction	Generating more reports or documentation than required by the regulator or board.	Monthly 100-page conduct reports when quarterly executive summaries meet the FSCA's impact tolerance.	• **Query:** Does every report produced serve a specific Board or Regulator requirement? • **Audit action:** List all recurring compliance reports and identify any that haven't influenced a strategic decision in the last 12 months. • **Lean goal:** Consolidated, executive-level "outcomes"-based summaries of key matters.

Waiting	Delays caused by slow internal sign-offs or "information silos" between Risk, IT, and Finance.	Waiting three weeks for IT to pull data for a sudden Prudential Authority (PA) request.	• **Siloed data access:** Does the risk or compliance team have to wait for the IT department or a business unit to "pull" reports from legacy systems?
			  • *Lean Goal:* Implement self-service dashboards that provide real-time access to core risk data without intermediary intervention.
			• **Sequential governance sign-offs:** Do regulatory filings or policy changes sit in an "inbox" waiting for sequential manual approvals from multiple committees?
			  • *Lean Goal:* Transition to parallel digital approvals or pre-authorised "threshold-based" sign-offs for routine filings.
			• **Third-party information gaps:** Are compliance reviews delayed because of slow responses from outsourced partners or vendors regarding their POPIA or cyber resilience status?
			  • *Lean Goal:* Use automated vendor risk management portals where partners must upload "demonstrable compliance" evidence directly into your monitoring system.
			• **Inter-subsidiary information latency:** Does the Group-level function wait days or weeks for African subsidiaries to standardize and submit their local risk assessments.
			  • *Lean Goal:* Use a "Local Adapter" reporting framework where subsidiaries input data into a shared cloud repository, allowing the Group to see aggregated risk levels instantly.
			• **Regulatory query response time:** Is the firm's response to an urgent Prudential Authority (PA) or FSCA query delayed because data needs to be manually cleaned or reconciled first?
			  • *Lean Goal:* Industrialise data quality controls at the source to ensure all regulatory-relevant data is "audit-ready" at all times.

Over-processing	"Gold-plating" a control by adding excessive steps that do not add protective value.	Running triple-manual reconciliations on a process that is already digitally validated upstream.	• **Query:** Are there manual controls on processes that are already digitally validated upstream? • **Audit action:** Review manual reconciliations in capital modeling and financial reporting streams. Determine if automated "system-to-system" validations can replace human sign-offs. • **Lean goal:** "One-touch" data flows from core systems directly to regulatory filing templates.

Waste Type	Definition in a Regulatory Context	2026 Example	Key Questions and Lean Actions
Inventory (backlogs)	Accumulating unreviewed alerts, un-filed returns, or obsolete data that obscure real risk.	A backlog of 5,000 low-risk AML alerts that prevents the team from seeing high-priority threats.	• **Query:** Is the compliance team buried in low-risk alerts (e.g., AML or transaction monitoring)? • **Audit action:** Analyse alert-to-suspicious-activity ratios. Identify thresholds where high volumes of false positives are obscuring real threats. • **Lean goal:** High-precision, AI-driven filtering that directs experts to only the most credible risk signals.
Defects (rework)	Errors in regulatory filings or data entry that require time-consuming correction and re-submission.	Re-submitting a capital adequacy calculation because of a manual spreadsheet error	What is the root cause analysis? Fix it for the long-term, don't solve immediate reporting need
Motion	Unnecessary movement of data or people between disconnected systems to complete one compliance task.	Manually copying data from five different subsidiary legacy systems into one Group report.	• **Query:** How many disparate systems must an employee access to complete a single "Know Your Customer" (KYC) file? • **Audit action:** Map the "distance" data travels across subsidiaries. Identify where manual "copy-pasting" occurs between legacy systems and the group reporting hub. • **Lean goal:** A centralised "Compliance Core" or data lake that serves as the single source of truth for all jurisdictions.

A proactive, intelligence-driven strategy

Lean Regulatory Risk Management is not about doing less compliance, but about doing smarter compliance. While cutting corners indiscriminately reduces protection, "lean management" reallocates effort from low-value, administrative "noise" toward high-impact, demonstrable outcomes that protect capital and consumers.

In the eyes of the Prudential Authority (PA) or FSCA, a firm that has "cut corners" lacks a robust risk culture, whereas a "lean firm" can clearly articulate—through its Regulatory Impact Assessment—exactly why specific resources have been prioritised to ensure that impact tolerances are never breached. Regulators appreciate targeted focus on key matters whilst demonstrating all requirements have been met.

In 2026, it is insufficient to state that you follow best practices. You must prove demonstrable compliance. Focus on the quality of evidence over the quantity of procedures. Appropriate managed, regulatory risk management is a fundamental part of a firm's operating strategy—not a cost center. By adopting Lean Regulatory Risk Management, firms can more efficiently satisfy a regulator's push for stronger risk cultures while simultaneously protecting the margins that are so hard-won in a stagnant macro economic environment.

Marius Botha

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

Key takeaways

- De-scope any control that provides zero impact on conduct outcomes or capital stability.
- Industrialise high-impact areas.
- Standardise core group policies while using "local adapters" for regional African subsidiaries.

Zaronia Transition

Zaronia Transition

A defining moment for transparency and resilience

In 2022, the Market Practitioners Group (MPG), a joint public and private-sector body comprising the South African Reserve Bank (SARB), the Financial Sector Conduct Authority (FSCA), and key market participants, designated the South African Overnight Index Average (ZARONIA) as the preferred successor rate to replace the Johannesburg Interbank Average Rate (JIBAR). This decision forms part of South Africa's broader benchmark reform initiative aimed at improving transparency, robustness and alignment with international best practice.

The strategic inflection point

The transition from the Johannesburg Interbank Average Rate (JIBAR) to the South African Rand Overnight Index Average (ZARONIA) is far more than a mandatory regulatory exercise. It is a strategic inflection point for South Africa's financial services industry. While the operational, legal, and risk management challenges are significant, a compliance-only mindset risks overlooking the profound opportunities for competitive differentiation, operational transformation, and market leadership that this transition presents. For the C-suite, the critical question is not *"How do we comply?"* but rather *"How do we capitalise?"*

Basis for the reform

The reform of major interest rate benchmarks forms part of a global regulatory response to well-publicised irregularities in the production of interbank offered rates (IBORs). Investigations revealed that these issues had persisted for years, including during the 2008 global financial crisis, when collusions among market participants in determining lending rates raised concerns regarding market integrity. The global financial system has since undertaken a multi-year transition away from LIBOR, with the process largely completed in 2023.

LIBOR's shortcomings highlighted broader structural weaknesses inherent in many IBORs. These included an over-reliance on expert judgment rather than observable market transactions, heightened vulnerability to manipulation, declining representativeness of underlying market activity, and limited resilience during periods of market stress. As a result, global markets have shifted toward more robust alternative reference rates (ARRs), particularly overnight near risk-free rates (ONRRs) which better reflect actual funding conditions.

Against this backdrop, global benchmark reform gained momentum, guiding the MPG's evaluation of ARRs for South Africa. The SARB deemed it prudent to plan for the discontinuation of JIBAR and transition toward a more resilient benchmark, ZARONIA.

Key distinctions: ZARONIA vs JIBAR

ZARONIA measures the interest rate at which commercial banks in South Africa obtain rand-denominated overnight wholesale funding in an environment where credit, liquidity and other risks are minimal. This low-risk requirement reflects the intention to anchor the benchmark in a deep unsecured overnight market, where risk is materially lower than in longer-dated transactions. ZARONIA is calculated using arm's-length pricing, actual unsecured overnight deposits of at least R20 million placed with commercial banks.

Eligible counterparties include commercial banks, non-bank financial corporates, non-financial corporates, and public sector institutions. Intra-group transactions are excluded, except those involving a bank's prime broking desk.

Commercial banks submit eligible transactions to SARB in line with prescribed reporting requirements. Using these submissions, ZARONIA is determined as a trimmed, volume-weighted mean of interest rates paid on qualifying deposits, rounded to three decimal places.

The SARB began publishing ZARONIA on 2 November 2022 to allow market participants to observe its behaviour and evaluate its suitability as a successor benchmark to JIBAR. The observation period concluded on 3 November 2023, after which ZARONIA continued as an official reference rate.

By contrast, JIBAR is a term reference interest rate that reflects the average cost at which South African banks are willing to lend unsecured rand-denominated funds to one another in the interbank market over specific maturities, most commonly the 1-, 3-, 6- and 12-month tenors. Unlike transaction-based benchmarks, JIBAR is derived from quoted rates submitted by a panel of contributing banks and intended to represent their estimated unsecured term funding costs. These characteristics mean that JIBAR incorporates term credit and liquidity risk premiums and are thus more susceptible to volatility during periods of stress. The table below highlights key differences between JIBAR and ZARONIA:

ZARONIA	JIBAR
Backward-looking overnight rate	Forward-looking term rate
Near risk-free rate and removes distortions caused by credit adjustments	Includes credit and liquidity risk premia, which may lead to hedge ineffectiveness
Based on actual unsecured overnight trades, reducing susceptibility to manipulation	Based on indicative quotes, not easily verifiable and susceptible to manipulation
All commercial banks contribute data, improving depth, liquidity, and market coverage.	Only five banks submit quotes, limiting resilience and representativeness.
Interest due is known only once the overnight rate is published – the interest payment is not known at the inception of the reset period.	Interest due is known at the start of the reset period, providing certainty about funding costs to assist with cash flow management.
Daily compounding can be operationally complex, requiring updated systems	Operationally simpler, as the rate remains fixed over the interest period (i.e., tenor)

Because JIBAR underpins a wide range of financial contracts, its successor needed to demonstrate robustness prior to market-wide adoption. The SARB undertook extensive back-testing using five years of historical transaction data sourced from the four largest commercial banks and the JSE. This assessment examined benchmark behaviour, validated parameters and evaluated the adequacy of contingency arrangements.

Results indicated strong data sufficiency and low volatility, except during the Covid-19 policy-rate shock, indicating that ZARONIA was robust and representative. Consistent with international experience, the back-tested ZARONIA rates traded below the repo rate, with an average spread of around 36 basis points, narrowing during Covid-19 due to monetary policy interventions. Importantly, ZARONIA responded predictably to repo rate movements, confirming its suitability as an effective monetary policy transmission mechanism.

Formal announcement of Jibar cessation

On 3 December 2025, the SARB formally announced that JIBAR would be permanently discontinued following its final publication on 31 December 2026. From that date, all JIBAR tenors will cease and be deemed non-representative for regulatory purposes. The SARB also fixed the Credit Adjustment Spread (CAS) for each tenor (for example, 0.1619% for 3-month JIBAR) providing certainty for fallback transitions. This spread will apply consistently to all exposures transitioning from JIBAR to ZARONIA post 31 December 2026.

At the time of publication, the transition should already be firmly underway. Market participants are expected to reference ZARONIA in all new contracts and to convert legacy JIBAR exposures before JIBAR's cessation. The next major milestone is the "No New JIBAR" date of 1 May 2026, after which no new JIBAR-linked contracts may be issued. This proactive cut-off reduces reliance on fallback triggers and mitigates operational risk at cessation.

The transition period

Given JIBAR's deep integration within South Africa's financial system, transition is inherently complex. Drawing on international benchmark reform experience, including LIBOR, the SARB structured the transition around three pillars outlining the critical milestones market participants must meet:

- **Pillar 1: Derivative market transition** – the transition begins with derivatives, as these instruments are structurally better aligned with near risk-free rates and therefore more adaptable to ZARONIA. This requires the entire ZAR interest rate swap market to shift from JIBAR-based swaps to ZARONIA-linked overnight indexed swaps (OIS), laying the foundation for a transition across other market segments

- **Pillar 2: Cash market transition** – because derivatives are often used to hedge cash-market exposures, the next step is extending ZARONIA to loans, bonds and money-market instruments. Cash markets typically transition more slowly due to product-specific and operational complexities, making standardised conventions essential for consistency and legal certainty. Once sufficient uptake of ZARONIA is achieved in new contracts, attention shifts to encouraging the conversion of remaining JIBAR-linked cash-market instruments

- **Pillar 3: Legacy contract transition** – the final pillar focuses on transitioning legacy contracts that will extend beyond JIBAR's cessation. Contracts without effective fallback clauses risk contract breaches once JIBAR is discontinued, making proactive conversion critical. To ensure economic neutrality, an adjustment spread must be applied to prevent contracting parties from being enriched or disadvantaged solely by switching to the fallback rate

Certain "tough legacy" contracts may not be amendable due to structural constraints. However, contractual continuity must be preserved through relevant legislative provisions enacted by the cessation date. Tough legacy exposures may include JIBAR-linked securities without robust fallback language, multi-lender loan agreements, bonds with high consent thresholds, exposures involving defaulted clients, structured notes, securitisations whose underlying assets reference legacy benchmarks, and long-dated infrastructure or concession-based financings, such as REIPPP and other PPP arrangements involving multiple parties.

Impact of the transition

The shift from JIBAR to ZARONIA has wide-ranging implications across contracts, systems, risk models, accounting frameworks and tax treatment.

Institutions should structure implementation around six integrated workstreams:

1. Strategy & Impact Assessment – Assess the organisation's full JIBAR exposure, quantify transition risks, and establish an enterprise-wide programme with clear governance. This includes defining a ZARONIA product strategy and creating an internal and external communication plan to educate stakeholders and ensure coordinated execution.

2. Legal & Contract Remediation – Draft new contractual provisions for ZARONIA-based products, amend legacy agreements, and embed robust fallback language. Entities must also understand anticipated legislative or regulatory measures that may affect tough legacy contracts requiring alternative treatment.

3. Risk, Valuation & Treasury – Manage valuation impacts, basis risks and economic equivalence during the transition. Develop updated valuation methodologies and modelling frameworks, recognising that swap curves, discounting approaches and JIBAR-based projections all require consistent conversion to ZARONIA.

4. IT & Systems – Implement changes to systems, data structures, infrastructure and processes to accommodate ZARONIA. This includes enabling daily compounding, updating pricing engines and ensuring staff have the technical skills required to operate in a ZARONIA-based environment.

5. Accounting & Tax – Disclose the impact of the transition to enhance investor understanding of the reform and ensure that accounting treatments (e.g., hedge accounting, practical expedients) align with tax considerations, including section 24J implications, capital gains tax effects, and the treatment of compensatory payments needed to maintain economic equivalence.

6. Programme Governance & Project Management – Coordinate and oversee all transition activities across the organisation to ensure an integrated, timely and well-controlled implementation. This includes setting a detailed transition roadmap, defining roles and responsibilities, tracking progress across workstreams, managing cross-functional dependencies, and escalating issues that could delay readiness ahead of the 31 December 2026 cessation.

An enterprise-wide approach is essential to ensure readiness well ahead of the 31 December 2026 deadline.

Seizing the Zaronia opportunity

The shift to ZARONIA is a catalyst for creating deeper, more transparent, and more efficient ZAR interest rate markets. Institutions that actively participate in this evolution can help shape the future market structure and position themselves to capture first-mover advantages. The practical implication is clear: entities should pursue an active transition now by migrating new business to ZARONIA, remediating contracts, upgrading systems and aligning accounting, tax and risk frameworks well ahead of 31 December 2026.

Those who approach this transition strategically will not merely comply, but they will help define the next chapter of South Africa's financial market infrastructure.

Ben April

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

Ferdinand Mokete

Partner
Financial Services
KPMG South Africa
T: +27 82 715 2840
E: ferdinand.mokete@kpmg.co.za

Key takeaways

- The ZARONIA transition is not a project to be delegated; it is a strategic imperative to be led from the top.
- Champion an opportunity-centric vision: Frame the transition not as a burden but as a catalyst for innovation and transformation.
- Sponsor strategic investments in systems and capabilities: Allocate the necessary resources to modernise technology, re-engineer processes, and develop new products.
- Empower cross-functional collaboration: Break down organisational silos to foster collaboration between trading, risk, operations, IT, and legal.
- Lead client engagement from the front: Personally engage with key clients to demonstrate commitment and strategic partnership.