KPMG

Ten key regulatory challenges of 2024

Strengthen the cards you hold

kpmg.co.za

Introduction

On behalf of KPMG's Africa Regulatory Centre of Excellence I am delighted to share our Ten key regulatory challenges for 2024.

Regulatory scrutiny continues to intensify in 2024. The economic outlook is challenging with upcoming elections, high inflation and prolonged periods of high interest rates creating uncertainty for shareholders and investors. The operating environment faces unprecedented threats, highlighting vulnerabilities across the business environment. Is your organisation playing the best they can with the hand they have been dealt? In an ideal world, increased budget and raised priority for regulatory spend would go a long way to mitigating these risks, however the current environment requires firms to be resilient and resourceful. Strengthen the cards you hold!

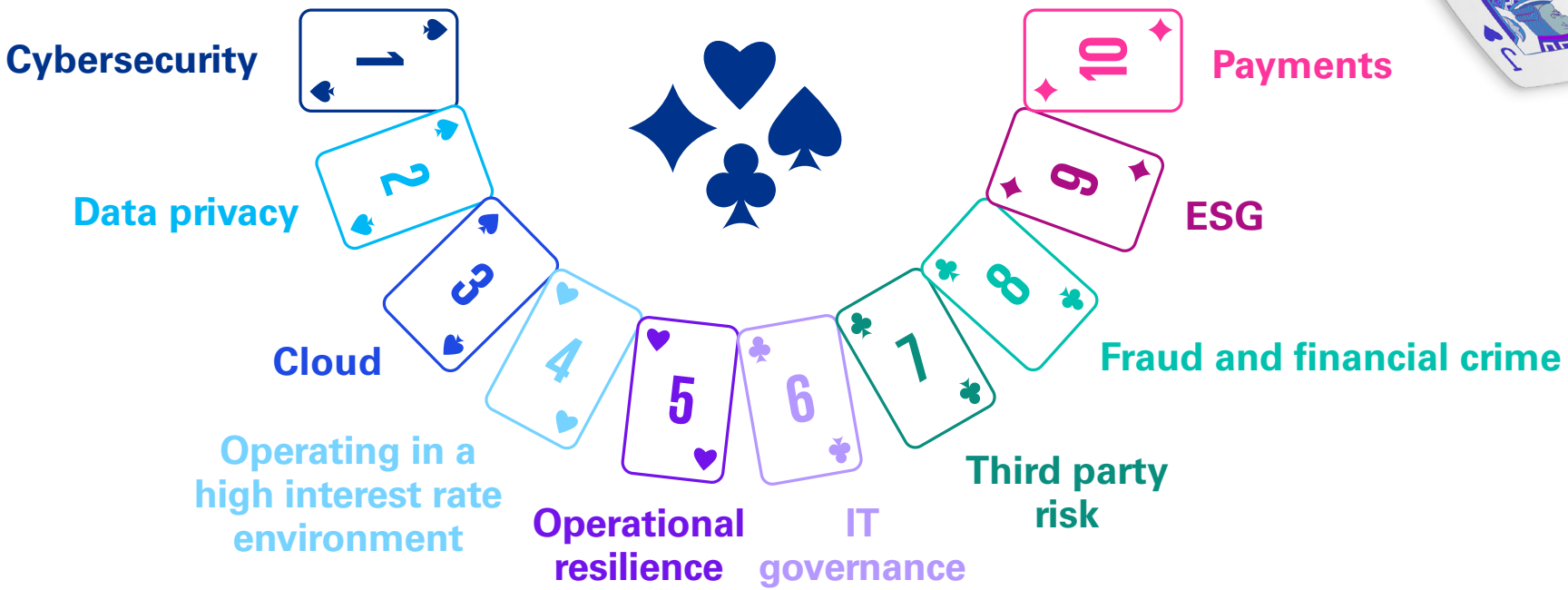
1. **Cybersecurity**
2. **Data privacy**
3. **Cloud**
4. **Operating in a high interest rate environment**
5. **Operational resilience**
6. **IT governance**
7. **Third party risk**
8. **Fraud and financial crime**
9. **ESG**
10. **Payments**

Please reach out to us should you wish to discuss any of our ten key regulatory challenges in more detail and deep dive into strengthening the cards that your organisation holds.

Michelle Dubois

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

Ten key regulatory challenges of 2024



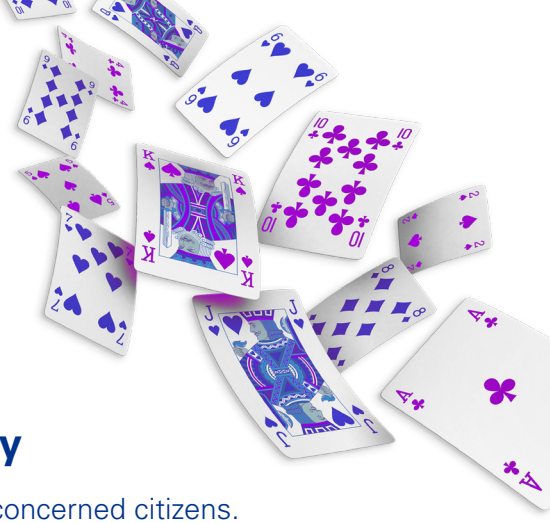
Technology and Data

Growth and Resilience

Risk Management and Governance

Environmental and Social

1 Cybersecurity



1 Cybersecurity

Building a resilient and trustworthy financial ecosystem is a social responsibility

Criminals are nothing if not creative and the same can be said for cybercriminals. One would not typically classify them as concerned citizens. Recently, a ransomware crime syndicate felt it was their moral obligation to inform that US Securities Exchange Commission ("SEC") when the victim of a ransomware attack failed to report the material incident to the regulators within four days, as required by law[1]. It is unfortunately no surprise that these upstanding members of society were in fact behind the attacks in the first place. This is an example of how pressure mechanisms have evolved over time. The more that organisations improve cybersecurity controls, the more syndicates find novel ways to make life uncomfortable.

In October 2023 the SEC announced that a US-based technology company along with its Chief Information Security Officer ("CISO"), would be charged for misrepresenting known cybersecurity risks and vulnerabilities – and failing to take appropriate action[2]. The incident in question, happened to be one of the largest supply chain cyber attacks in reported history. The SEC charges that the CISO failed to sufficiently raise known cybersecurity issues within the company. Following the cyber attack, the organisation did not completely disclose the full nature and impact of the incident. Ultimately, a negative ruling for the organisation will likely further damage their severely impacted reputation while imposing fines and bar the CISO from holding senior positions in future.

Closer to home

It is clear that regulators are increasingly pushing organisations in strategically important industries like energy, finance, and health care to be cyber resilient and position themselves to be able to recover from major incidents. The focus is just as much on resilience (or ability to recover from an incident) as it is on confidentiality (information protection) and integrity (information accuracy) to complete the circle (or triangle if you will). The Digital Operational Resilience Act ("DORA") in the European Union is a prime example of this. What does this mean for us at the Southern tip of Africa?

Following on the heels of the Protection of Personal Information Act and the Cybercrimes Act, the Financial Sector Conduct Authority ("FSCA") and South Africa Reserve Bank Prudential Authority ("PA") released the Draft Joint Standard on Cybersecurity and Cyber Resilience for comment in 2021[3]. While the standard was earmarked for a 2022 release, delays in these matters are both expected and in some cases, required, to ensure appropriate consultation with industry. While no updated concrete publication date have been communicated, we can expect final issue in the not too distant future.

Draft Joint Standard – Cybersecurity and Cyber Resilience

The standard states that it is meant to "address requirements relating to governance, cybersecurity strategy and framework, cybersecurity and cyber resilience fundamentals, cybersecurity hygiene practices, as well as regulatory reporting". It applies to most financial institutions ("FIs") including banks, insurers, investment managers, and more. However, the regulatory buck does not stop there and will include third party service providers.

The standard does leave room for flexibility in the application of the standard. FIs can implement the requirements of the Joint Standard in accordance with "risk appetite, nature, size and complexity of the financial institution". Naturally larger corporates will have considerably more resources to enable compliance when compared to smaller firms. Fair warning though – it is not a get out of jail free card so expect the regulator to rigorously test the interpretation and application of this clause.

[1] Ransomware group reports victim it breached to SEC regulators | Ars Technica

[2] SEC.gov | SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

[3] Draft Joint Standard - Cybersecurity and Cyber Resilience (resbank.co.za)

Some of the key highlights of the standard:

Strategy and Governance: The Joint Standard crystalises the role of the organisational governing body (board and senior management) to hold the ultimate responsibility for compliance with the Joint Standard, in addition to the oversight of cyber risk management in general. Expect to see cybersecurity as a standing agenda item in senior leadership meetings, if not already there. Clear roles and responsibilities with multiple lines of defense embedded, is a must. A clear and risk-focussed approach to combined assurance will be important to ensure compliance. FIs will be required to demonstrate a comprehensive and risk-informed strategy and control framework to combat cyber threats, which is aligned to the strategic direction of the business. The strategy must be operationalised through supporting policies, procedures and standards – and importantly – subject to regular independent review.

One area where we expect to see challenges is the expectation that security governance and oversight must be independent from security operations. This essentially means that the same person ensuring that your IT security technologies (firewall, anti-virus, etc) are configured optimally, cannot be the same person providing cybersecurity oversight. This requirement casts the role of cyber and information security governance as a Second Line function in stone – in line with most good practice standards and guidelines worth its salt. In many organisations, in particular smaller FIs, it may present a challenge to create the structures necessary to support the level of independence expected due to legacy reporting structures and resource requirements.

As with DORA, the Joint Standard places an emphasis on third-party service providers, requiring financial institutions to "ensure that IT systems managed by third-party service providers are accorded the same level of protection and subject to the same security standards". Given the introductory example on the importance of a cybersecure supply-chain, it is no wonder regulators are casting their nets as widely as possible.

Cybersecurity and cyber-resilience fundamentals

Section 8 and 9 of the draft Joint Standard get to the heart of the matter, with requirements categorised under: Identification, Protection, Detection, Response and Recovery. This follows a pragmatic approach towards building a comprehensive control set not too dissimilar from well-known industry security standards. We expect most FIs to have these technology and process requirements largely in place, perhaps working towards a more consistent application thereof.

Any good cybersecurity compliance programme will ensure that critical operations and information assets are prioritised for protection - throughout the information lifecycle. The human factor is certainly not ignored, however it is no longer enough to only complete your annual phishing training and regard this requirement as completed. Crucial emphasis is placed on the governing body to ensure that they are armed with enough knowledge and awareness to execute their oversight mandate effectively.

Another area of particular importance is the organisation's ability to detect a cybersecurity incident in order to effectively respond. We have found "Purple Team" assessments particularly useful to test your security operation's ability to detect and respond to attacks. A Purple Team Assessment is an approach whereby the Red Team (the offensive team) and the Blue Team (security operations) are integrated into a collaborative approach to "wargame" agreed upon attack paths. Moving beyond pure table-top exercises, the joint effort promotes a culture of continuous improvement, breaking down silos and enhancing communication towards a proactive and security-conscious mindset. Given that many organisations outsource their security operations centre ("SOC"), it aids in obtaining the necessary comfort that service levels are at expectation, in addition to being a practical application of your third party risk management programme.

Naturally, the standard stresses the importance of a strong backup and recovery plan to ensure that IT systems can be recovered in the event of an incident. It states that backup media must be stored offline "or" at an offsite location. Given that cybercrime syndicates have become adept at sniffing out any network connected backups, we expect this clause to include further requirements to ensure that connected backups are stored in an immutable state even if kept offsite once published in final form. This will ensure that ransomware operators are unable to alter backups during the encryption phase of a ransomware attack.

Cyber Hygiene: Hygiene expands on many of the core "bread and butter" cybersecurity processes without which perfect strategies, policies and procedures essentially are null and void. This includes vulnerability and patch management, access management, malware protection, secure configuration and more – collectively known as Attack Surface Management[4]. This is where, in our experience, failures most often occur. How often does the business imperative to keep the lights on at all costs override an ever-growing list of undeployed patches? There is a notion that, as cybersecurity professionals, we have to get it right every time – a hacker just needs to get it right once to compromise the organisations environment. And getting cyber hygiene right consistently will potentially be the biggest challenge in complying with the Joint Standard.

Regulatory Reporting: In addition to regularly compliance reporting, the Joint Standard requires FIs to report material incidents within 24 hours of classifying the incident as such. This crucial point is worth noting and should be highlighted in your incident response framework.

The responsibility of cybersecurity

The introduction of the Joint Standard represents a crucial milestone for the industry and it must be viewed as "more than just compliance for the sake of it". It addresses the pressing need for enhanced cybersecurity measures to build a more resilient and trustworthy financial ecosystem as a social responsibility. Compliance serves as a proactive approach to risk management, instilling confidence among industry stakeholders and the public; while reinforcing good governance. Regulators around the world are taking it seriously, and so should we.

Gustav d'Assonville

Cyber Strategy & Governance Lead
KPMG South Africa
T: +27 66 304 2062
E: gustav.d'assonville@kpmg.co.za

[4] Enhancing Cyber Defence: Trends in Attack Surface - KPMG UK

Key Actions

- Cyber Risk Quantification is a crucial aid in supporting compliance by providing a precise understanding of threats, enabling informed decision-making.
- Continual assessment, mitigation and monitoring of risks associated with external partners are a pivotal part of compliance.
- Ensure that your attack surface management is operating as expected with consistent cyber hygiene practices.

2 Data Privacy

2 Data Privacy

International Transfers – Regulatory compliance may not be enough

We live in a world where technology connects people and blurs geographical boundaries. As a result, data has become an invaluable asset for individuals and organisations alike. Businesses are rapidly transforming and the world is becoming smaller in this digital era. However, the expanding global network of data sharing raises concerns about data privacy and protection, particularly when personal information is transferred across borders. Regulators across the globe are trying to "play catch up" to ensure that their privacy laws and regulations best protect data subjects amidst the evolving commercial needs of organisations.

As organisations increasingly engage in international transactions, understanding the risks and regulatory requirements surrounding data privacy becomes crucial.

There is a business need to transfer data seamlessly across borders

Organisations need to transfer data (which often includes personal information) for various reasons. Market expansion is a natural product of a thriving organisation. With increased access to foreign customers, and reduced barriers to entry into foreign markets driven by digital trade, follows the demand for the free flow of information across borders. Technology has certainly enabled organisations to extend their reach beyond their geographical borders like never before. As a result, organisations are increasingly required to transfer data not only between their various offices but also to international partners and foreign service providers.

Multinational organisations routinely exchange data across related companies including foreign companies. Such international transfers allow multinational organisations to optimise their operations by creating efficient cost centres, foster collaboration and creativity within the group, and allow businesses to analyse international trends and capitalise on opportunities.

More and more local companies are considering cost optimisation strategies through their supply chains. This often involves outsourcing specific activities to foreign service providers to enhance efficiencies and optimising resources to remain competitive.

The international transfer and storage of data plays an important role in the strategy of disaster recovery by dispersing data across several locations around the world. Dispersing data across several locations can support in safeguarding critical data and allowing for swift recovery and continuity of business operations where one location may be compromised or subject to a cyber attack.

Regulatory challenges faced by business

Coupled with the demand for free flow of information across borders, comes a sharp rise in regulations and legal frameworks which seek to limit the unfettered transfer of personal information internationally in order to protect the fundamental rights and freedoms of data subjects.

Disparate laws pose a real challenge for companies wishing to do business internationally. Consider the circumstances where your company is established in a jurisdiction, like South Africa, that has robust data privacy and protection laws, but there is a real business need to engage with a third party established in a jurisdiction with no data privacy laws and regulations. How can you adequately manage that risk to personal information collected from your customer or employees? Will your legal team be able to negotiate strong contractual terms with the service provider? What is considered sufficient from a South African data privacy law perspective? What value is the contract in circumstances that the service provider's local laws allow for excessive government surveillance or otherwise undermine the obligations in the agreement. It becomes increasingly difficult for South African companies to confidently transfer personal information internationally without considerable research and assessment into the laws applicable in that jurisdiction.

It is no surprise that increasingly, regulators are requiring companies do more to mitigate against the risks associated with international transfers of personal information. On the one extreme, some regulators are banning the transfer of personal information outside of the country of origin. Other jurisdictions allow the international transfer of personal information subject to certain conditions or controls being implemented (e.g. contractual agreement, assessment of adequacy of foreign laws etc). Although, the regulatory requirements may differ from one jurisdiction to another, the intention remains the same – protect personal information when it is transferred outside of our jurisdiction.

Is compliance enough?

From a South African perspective, international transfers of personal information are prohibited in unless an exception contained in section 72 of the Protection of Personal Information Act, 2013 ("POPIA") is applied. However, the application of these exceptions in a South African context is still untested and subject to the interpretation of each organisation. Some of the questions that organisations are grappling with are:

- How does the organisation assess whether the laws of a foreign country provide "substantially similar" protection to the laws of South Africa? Who should perform the assessment? What level a similarity is acceptable?
- Will the conclusion of strong data privacy provisions be sufficient when the organisation is aware that the third party is unable to comply in terms of its local laws?
- When requesting the data subject to consent to the international transfer of personal information, should the organisation have disclosed that the organisation has not assessed the laws of the foreign jurisdiction or that the third party has not contractually agreed to robust data privacy obligations?
- What does the organisation do when a data subject withdraws his/her/its consent to international transfers?

Relying on any one of the mechanisms set out in section 72 of POPIA allows a South African organisation to compliantly transfer personal information internationally. However, "doing the bare minimum" may not be enough and certainly does not guarantee the loyalty and satisfaction of customers / employees whose information was not protected in the foreign jurisdiction. Some data subjects may even argue that whilst the organisation was legally compliant, it was nevertheless negligent to transfer personal information to a jurisdiction without data privacy laws particularly where the data subject wasn't informed of this risk at the outset.

The need to remain agile, adaptable and interconnected

In an interconnected world, fluidity and the ability to access and transfer information (including personal information) across markets is no longer simply a desire but a real business imperative. We recognise that businesses need to remain agile and adaptable in the changing environment, and that organisations may not be able to wait for regulatory guidance or precedent on the matter of international transfers. However, it would be prudent for organisations to view international transfers from a business perspective rather than a mere compliance perspective.

It is important to assess the real risk of the international transfer even when meeting minimum regulatory requirements. Consider, what will the trust index of your company be after a shareholder's / customer's / employee's personal information is accessed by government authorities without a fair judicial process? Will you be able to retain existing staff or customers who discover that the third party's contract is not worth the paper it was written on following a security breach? What is the potential impact on your organisation's reputation?

It may be helpful to have regard to the requirements set out in other countries' laws when transferring personal information across your borders. This may provide you and your data subjects with comfort that the best possible protection mechanisms are being implemented when transferring personal information abroad.

Farah Jakoet

Legal Senior Manager
KPMG Law
(a business unit of KPMG Services(Pty) Ltd)
T: +27 66 474 2780
E: farah.jakoet@kpmg.co.za

Zizi Dlamini

Legal Manager
KPMG Law
(a business unit of KPMG Services(Pty) Ltd)
T: +27 72 251 2972
E: zizi.dlamini@kpmg.co.za

Key Actions

- Assess the real risks associated with the international transfer of information against the data privacy regulations of the countries involved in the transfer.
- View international transfers from a business perspective rather than a mere compliance perspective.
- Have a clearly defined process in place for when a data subject withdraws consent to international transfers.

3

Cloud

3 Cloud

Cloud perspectives in Africa

Cloud service adoption continues to grow worldwide, with the top three cloud providers in the world forming part of the world's top five companies by market cap. Cloud provides three service models, namely Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS") and Software as a Service ("SaaS"). The market size, as of 2024, for IaaS is USD 196 billion, PaaS at USD176 billion and SaaS at USD167 billion, continuing to grow as a foundation for technology and digital backbone.

Cloud is a key enabler for digital transformation journeys across the African continent. The growth has allowed for large investments from established hyperscaler cloud providers and localised cloud infrastructure providers to enable services across the continent and within local geographic regions. Cloud has helped support the development of digital skills, and provided new job opportunities, at times driven through regulatory efforts to drive local job creation and skills through data protection, outsourcing and cyber security regulations. It is important when adopting cloud services, to ensure compliance and regulatory requirements are understood and achievable by the cloud service provider, along with the ability to meet on-going regulatory changes.

An Africa perspective

For financial services organisations operating within a single or multiple jurisdictions in Africa, it is important to understand the evolving regulatory landscape and guidelines shaping the current and future of cloud adoption.

The South African Reserve Bank's Prudential Authority ("PA") has published guidance providing key principles for interpretation. This has allowed the financial services industry to take a principle based and risk based approach to cloud computing adoption and data offshoring. Though the PA has no specific requirement for regulatory approval, information related to material cloud computing and data offshoring agreements need to be provided, and any additional uncertainty can be consulted for further clarification. As many of the risk factors relate to data assets and residency, it is therefore a requirement to have a well-defined, board approved data strategy and data governance framework. In addition, policies, processes, access controls and frameworks are required to enable governance for cloud data assets for hosting, in conjunction with other regulatory requirements such as POPIA.

The Central Bank of Nigeria ("CBN"), the National Insurance Commission ("NIC") and the National Pension Commission ("NPC") agree that across the financial services industry in Nigeria, there are no specific cloud regulatory requirements. The CBN does recommend that banks comply with the IT Standards Blueprint, which covers overarching IT governance and provides guidelines which inherently need to be considered with cloud adoption. The CBN requires information, at any time, to fulfil its supervisory role, therefore having a well defined strategy, maintained documentation and reporting is important to ensure transparency for the cloud environment as part of audit reviews. In addition, other regulations are still valid and need to be considered as part of cloud adoption, including the Nigeria Data Protection Regulations ("NDPR"). The NDPR outlines that personal data should not leave the borders of Nigeria, but permits exceptions based on meeting the requirements outlined by the adequacy of protection and derogations.

Similarly Kenya and Botswana do not require regulatory approval, however there are general requirements for third party cloud service providers to comply with, as well as legal and regulatory framework requirements and global best practices. Cloud service use is part of technology risk, and therefore there is a general requirement to have a process for risk assessment and management. In Kenya the published cybersecurity guidelines notes (2017) and prudential guidelines on outsourcing (2013) would need to be adopted as part of cloud service adoption. These guidelines and principles cover requirements associated with risk management, due diligence, business continuity, monitoring and management. In addition, the Data Protection Act outlines guidelines on managing certain data assets which may restrict the use of cloud in certain use cases.

In Botswana the Data Protection Act ("DPA") and Guidelines on Cybersecurity and Resilience will apply and limited regions are accepted for public cloud hosting services, subject to consultation and approval from the Prudential Authority.

The Bank of Mauritius ("BOM") offers a slightly different and more mature perspective providing guidelines on the use of cloud services and outlines the requirements for banks to adopt cloud services. Cloud service use is permitted in Mauritius, provided the due diligence requirements are complete, including a strong focus on governance practices and risk management. There are requirements such as a board approved cloud strategy, exit strategy, governance frameworks and risk management practices which must all be met. In addition, the regulatory environment demands certain requirements for the third-party cloud service provider including a proven track record and ability to assess the cloud data centres.

The Bank of Namibia issued regulatory guidelines for outsourcing in banking institutions and cloud computing. The responsibilities require the board of directors to ensure outsourcing policies are comprehensive, support risk management, provide internal controls and oversight of third parties, that compliance measures are met by third parties and that external audits are supported through access to third party information required. Senior management are required to fulfil risk management, outsourcing party governance and monitoring for regulatory and compliance changes. The outsourcing policy and strategy, along with the risk management and governance processes need to be sound to successfully leverage cloud services.

Consider, architect and implement cloud

Though the benefits of cloud are well understood, and global adoption continues to grow within the continent, there are challenges which have resulted in slower growth, such as skills and enabling infrastructure in Africa. As we overcome these, cloud will continue to be a key competitive enabler for financial services. Cloud service providers have aligned to supporting local regulatory needs, offering robust security and compliance solutions, enabling operational efficiency, providing data-driven decision making, and access to innovation of new technology faster. Understanding the regulatory requirements, and having comprehensive planning through a cloud strategy, governance frameworks, risk management practices and oversight will steer many territories into a position to adopt and gain the benefits of cloud computing services.

Vinay Patel

Associate Director
Digital Consulting
T: +27 66 301 9184
E: vinay.patel@kpmg.co.za

Key Actions

- It is important to consider regulatory requirements upfront, therefore as part of your enterprise cloud strategy, ensure to assess and consider the regulatory landscape of operating geographies, along with the associated risks.
- Understand what services / solutions are available to meet your regulatory challenges. Cloud continues to evolve, new services and hybrid solutions continue to adapt to new market needs, and effectively support operationalisation.
- Conduct reviews on your technical environment to ensure the strategy and governance set are in practice and configured in alignment to the regulatory requirements.

4 Operating in a high interest rate environment

4 Operating in a high interest rate environment

Operating in a high inflation, high interest rate environment for a prolonged period

South Africa is currently facing a repo rate of 8.25 percent, and a prime lending rate of 11.75 percent, which is far higher than the average repo rate of 6.9 percent experienced over the past twenty years. The current level of interest rates has been termed restrictive by the South African Reserve Bank ("SARB") in that it presents a level that imposes a disincentive on business to borrow for purposes of investing in their businesses as well as a disincentive on consumers to borrow for consumption purposes. The intended consequence of the elevated level of interest rates is to reduce aggregate demand for goods and services in order to reduce the level of inflation facing the economy.

Interest rates are therefore elevated in order to reduce the high levels of inflation and inflation is elevated for a number of reasons, some of which extend back to the Covid-19 pandemic and even prior to the pandemic. The result of the pandemic on international prices of goods and services was large and can be attributed to the consequences of the restriction of movement of people and goods in order to slow the spread of the disease. Lockdowns of cities, and in some cases countries, that formed important components of international supply chains meant that the unrestricted movement of goods and services were impacted. This in turn created shortages of many different goods in many parts of the world. The result of these shortages was and upward pressure on the prices of a broad range of goods and services. At the time, analysts assumed these price increases would be transitory, since once the disease was contained and markets could trade normally again, the expectation was that supply chain efficiency would be restored and price pressures would be reduced and so to inflation. However, due to the duration of the pandemic and inactivity of many sectors while under different stages of lockdown, business in general experienced much financial pressure with many unable to continue operation. This meant that the actual markets for many goods and services as well as those supply chains had been disrupted and remained this way even once vaccines had been developed that allowed economies to reopen their borders and begin operating as they had done pre-pandemic.

Then in 2022, to complement the Covid-19 supply chain impact on prices, Russia invaded the Ukraine. These two markets were important global suppliers of two broad categories of goods: fossil fuels and a number of cereal based foods. The war in the Ukraine therefore caused a disruption in the markets for fuel and foods as well as related goods such as fertilizers and cooking oils and caused the prices of these and related goods to increase across the globe. Since fuel and food markets impact nearly all other markets either directly or indirectly, the impact on global inflation was dramatic with most regions experiencing levels of inflation not experienced for many decades and with no sign of the war abating, it would require an extended period of time in order for markets to either establish alternative sources of supply or find substitute products for those in short supply.

In response to the record inflation rates experienced around the globe, which erode people's wealth and earnings, central bankers hiked interest rates and tightened monetary policy in order to reduce aggregate demand and thereby cool their economies in order to reduce the inflationary pressure. As a consequence, over 2022 and 2023, interest rates also reached decades high levels and led to the situation we currently find ourselves in.

High interest rates present business a problem with respect to investment spending. Businesses can be seen to have a list of potential projects that focus on generating business growth, cutting costs and improving efficiency, with each of these projects creating a potential return on that investment. In order to decide whether to implement a particular project or not, the business owner needs to compare the return of that project to the cost of the particular investment, which is usually closely related to the prevailing interest rate. Therefore, as interest rates rise, fewer investment projects become financially viable since the costs of those investments rise along with the interest rates, while the return from those investments remains relatively fixed. On aggregate therefore, for all businesses in the economy, as interest rates increase, investment expenditure tends to decrease and decades high interest rates would potentially also result in low investment spending.

Furthermore since investment spending forms an important part of a country's gross domestic product (GDP), one can expect lower economic growth at best and potentially even a contraction of the economy if this reduction in spending along with private consumption spending is severe enough. Lower economic growth can then lead to lower revenues and earnings growth, with even less money for growth, and expansion projects resulting in even lower economic growth in future, which can become a vicious cycle until interest rates moderate.

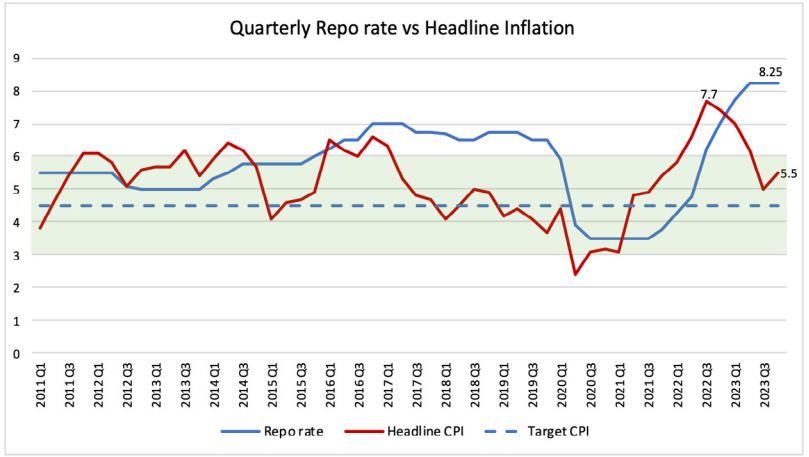
An alternative view of the impact of high interest rates on a business is to focus on the impact on cash flow. As interest rates rise, a business would be faced by growing debt service costs, which would divert cash from savings, if these were available, as well as other areas of the business focusing on growth, efficiency or sales to servicing debts. Additionally, the longer the business had to face high levels of interest rates the more vulnerable it would become to external shocks since any additional impacts in terms of breakdowns, maintenance costs, loss of sales etc would compete for those cash flows needed to service debts and therefore impact its continued operation. More extreme scenarios could result in the business unable to generate enough cash to service its debt over an extended period of time, putting it into default.

Looking ahead for some relief

During times like these it is thus vital for the business to preserve cash and reduce costs in order to not only maintain its normal operation in light of its additional debt servicing burden, but also to create a buffer to further economic shocks that could impact the business over this period. As a consequence of the required austerity, business spend less and consequently contribute to further shrinkage of the economic activity until interest rates moderate.

To date, South Africa has experienced a gradual reduction in its inflation rate from the highs of 7.8 percent in July 2022 to the most recent 5.1 percent in December 2023 and the expectation is for inflation to continue to moderate through 2024 towards the target rate of 4.5 percent. This reduction in the inflation rate will allow for interest rates to be reduced from the current restrictive level to a more investment and growth supportive level by the end of 2024 or early 2025 which will be good news for business in particular and the country in general. This is expected to contribute to faster economic growth.

It is, however, important to note that the current state of the economy is not only determined by the current level of interest rates, but also by additional factors including political uncertainty, inconsistent policy as well as the presence of inefficiencies in the economy including the continued electricity supply constraint, as well as deteriorating logistics infrastructure including the state of ports, rail and road infrastructure. Consequently, a reduction in inflation and interest rates may only have a marginal effect on the growth prospects of the economy, which would require substantial restructuring in order to be growth supporting. However, the expected reduction would be expected to provide a degree of financial relief and offer business more options in terms of pursuing their growth strategies.



Source: StatsSA, KPMG analysis

Frank Blackmore

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

Key Actions

- Provide for interest rates to normalise in small increments over an extended period.
- Preserve cash and cut unnecessary costs.
- Revisit diversification options for revenue streams.

5 Operational resilience

5 Operational Resilience

Redefining resilience

After the global financial crisis, regulators and organisations placed a key focus on financial stability as the crisis demonstrated to regulators that a financial collapse at one organisation could threaten the operational resilience of the entire system. The learnings led to regulators issuing a number of directives within their jurisdictions and working with the industry to mitigate the risk. Over the past decade, whilst a strong focus on financial stability still remains, it has been evident that risks are ever evolving and multi-dimensional, with disruption related risks now extending to potential events that would not have been identified in the past. This has resulted in a shift back toward operational resilience. Recent events such as the pandemic, the outcomes of which the world is still recovering from, have made it clear that low likelihood, high impact events are happening more frequently.

The importance of mapping interconnections and interdependencies

The year 2023 brought heightened fears over the potential collapse of South Africa's electricity power grid, which would have caused widespread economic pressure, in addition to impacting some 60 million citizens, their safety and security. Although the risk did not materialise to date, organisations rapidly turned to their business continuity programmes to understand their level of preparedness and establish contingency plans in the event of a total blackout. Ongoing loadshedding continues to test resilience capabilities. To some, it would seem that that a total blackout in South Africa would largely impact only South Africa, however, some neighbouring countries purchase power from South Africa and also rely on essential goods which make their way from the country's seaports. Taking this example into consideration demonstrates the importance of mapping interconnections and interdependencies, which are crucial in ensuring that any resilience programme is robust and accounts for all stakeholders that may be impacted in disruptive times.

Direct versus indirect impact

Typically, risk and business continuity practitioners tend to concentrate on risks with direct impacts due to the consequences of such risks arising, however, global events are swiftly shaping the risk landscape of countries, regions, and organisations. The 24th of February 2024 marks the two year anniversary of Russia's invasion of Ukraine. The war continues without any concrete sign of reprieve on either side.

Ukraine and Russia dominate agricultural exports around the world, representing more than half of global trade in sunflower oil and almost a third in wheat. Due to the ongoing war, an increase in food prices has been felt across many large African nations that depend on direct imports from these countries. Aside from the risks in the supply chain, food insecurity may lead to social unrest, ultimately causing damage to key infrastructure. South Africa is vulnerable to this, given the riot and flooding crisis that was experienced. This re-emphasises the importance of planning for continuity of operations and increasing our ability to become resilient with each passing day as we face unprecedented times ahead.

Global regulatory intervention

Regulators have been making their intentions clear. The Bank of England has been active in promulgating regulation on operational resilience, followed by the other developed economies which are sharpening their focus on enhancing existing operational risk regulation. This extends to emerging markets such as South Africa, with the South African Reserve Bank's Prudential Authority ("PA"), publishing Directive 10 of 2021 on 14 December 2021, Principles for Operational Resilience. This directive emerged on the back of the Basel Committee on Banking Supervision ('BCBS") paper on the same topic. A fair amount of effort is still required within Africa to establish effective programmes on operational resilience which are well understood, implemented and sustainable in addition to addressing the evolving regulatory requirements.

Understanding operational resilience

The meaning of "operational resilience" is not uniform globally, and especially within the African region. The Business Continuity Institute ("BCI) published the results of the Africa Region Survey on Operational Resilience in May 2023. The results indicate that there is still confusion as to how to implement operational resilience, how traditional business continuity practices play a role and its differentiation from organisational resilience. In addition, most organisations in the banking and finance sector stated that regulatory requirements are the main motive for having an operational resilience programme in place.

Some of the major challenges in implementing operational resilience within organisations include:

- Not having a good understanding of operational resilience and how it differs and supplements other business continuity and resilience programmes;
- Lack of an overarching framework or guideline which clearly articulates "how" to implement operational resilience, sustain it, and continuously enhance it;
- Lack of guidance from regulators surrounding the detail behind requirements to enable organisations to comply;
- Convincing management of the importance of adopting operational resilience; and
- Not having the capacity and/ or skills to implement a realistic policy.

Whilst this list of challenges is not exhaustive, they represent the immediate challenges which need to be overcome in a manner which enables organisations to move forward with clear intent and the ability to implement an operational resilience framework confidently. The PA's directive states that all banks must comply with the respective requirements specified, on or before 31st December 2024. This gives institutions less than a year to establish a robust framework and demonstrate their ability to comply. With this in mind, it is of paramount importance to refresh the understanding of operational resilience. "Operational Resilience" is defined as the capacity of an organisation to anticipate, prepare, respond, adapt, recover, and learn from business disruption. It is also considered as an outcome that benefits from the effective management of operational risk. For this reason, being well informed and guided by a holistic framework is critical.

The strategic advantage of resilience

Even though regulatory compliance is a key driver in embedding operational resilience, organisations should look to the practice as a mechanism for ensuring continuity of important business services and:

- Understanding, monitoring, and managing disruption related risks;
- Defining impact tolerances for important business services;
- Choosing plausible scenarios for testing;
- Demonstrate the ability to deal with disruptions and stay within impact tolerances;
- Mapping important business services to a level which allows for the identification of vulnerabilities and threats;
- Embedding a culture of resilience within the organisation across people, process, and technology; and
- Increasing stakeholder confidence by reporting and learning from disruptions.

Questions surrounding the required investment and how to leverage currently established practices are forever being asked by practitioners and senior management, with several opposing views regarding the right path to take. As with any new programme or framework, a gap analysis or current state assessment ("CSA") is recommended as a starting point to identify what is required and what may be leveraged. Many organisations are now exploring how they might 'power' their resilience efforts forward and achieve material advantage by connecting existing tools, technologies, and data sets into a cohesive whole in order to bring proven methodologies and acceleration catalysts to their programme. Rather than attempting to catalyse change in narrow siloes or distinct processes, the leaders are connecting their technologies and processes to drive more fundamental outcomes. Operational resilience is not about re-inventing the wheel but more so an opportunity to bring together several focus areas into a holistic, all-encompassing approach that ensures the continuation of important business services.

It is easily forgotten that with risks, come several opportunities. By making a concerted effort in achieving operational resilience, organisations will increasingly enable greater synergies across strategic, financial, and operational resilience together with enhancing stakeholder trust and reducing operational risks to a level which is acceptable and within impact tolerances. Risks are no longer on the horizon but creeping up onto our doorsteps without warning, which makes the case for redefining resilience in a manner which is consistent with leading practices and within the context of the organisation.

Manesh Purshotam

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

Key Actions

- Embed resilience into the culture of the organisation by having a resilience mindset in everything you do.
- Perform a gap analysis or current state assessment to understand where your vulnerabilities lie as an organisation.
- Conduct simulation exercises to test your organisations readiness to cope with disruption.

6 IT governance

6 IT governance

IT Governance – the lifeblood of the organisation

John Chambers, the former CEO of CISCO Systems said "Corporate Governance is like oxygen for a company, it is essential for survival and growth". If Corporate Governance is like oxygen, then IT Governance is like blood – because it needs to flow through every part of the organisation, carrying oxygen and critical nutrients (i.e. complete and accurate data) to all parts of the company. In the same way that blood is crucial for a human to live, IT Governance is crucial for all organisations and industries to ensure that technology risk is appropriately managed.

In order to assure stakeholders that:

- IT systems and data are secure,
- that integrity of data and systems is preserved and
- that value is derived from the substantial investment in technology.

What is driving the need for IT Governance?

Technology risks impact across the enterprise risk spectrum and given the rapidly evolving landscape of technology, accelerated pace of technology adoption in areas such as cloud and AI, and increased use of third parties, technology risks are increasing rapidly AND becoming more complex to mitigate. Some of the critical IT risks which organisations are grappling with, include emerging technology risks such as AI and blockchain, obsolete technology and cyber security risks. In addition, the capital markets and stakeholder expectations over the level of disclosure that companies provide and therefore what needs to be assured, is also evolving.

With the introduction of the Integrated Report, we have already seen that companies are required to disclose not only financial results, but also the organisation's strategy, governance, performance and prospects. We believe that stakeholders will be looking for more disclosure on technology and how technology is being used by the organisation, not only to run the business, but as a differentiator, driving us to a future assurance landscape of potential unlimited assurance.

Regulatory evolution

Regulatory focus on technology has evolved over a number of years. As far back as 2010, the focus was on data governance with the issuing of various financial reporting standards, regulatory standards and regulations being released related to data quality. Over the years we saw a shift to cybersecurity, cloud and third party risk and in 2018 driven by GDPR and POPIA the attention turned to information protection and privacy. Recently, the focus is on responding to the risks posed by and regulating crypto, AI, operational resilience, data regulations as well as global standards on ESG with the likes of the Digital Operational Resilience Act ("DORA") and the Digital Markets Act ("DMA") being release further afield.

The FSCA and PA in South Africa have recently released Joint Standard 1 of 2023 (IT Governance and Risk Management for Financial Institutions, 2023). The standard sets out the principles and minimum requirements for IT governance and risk management that financial institutions must adhere to. One key attribute clearly highlighted is the responsibility of the "governing body" of the financial institution to ensure that the organisation meets the requirements of the Joint Standard on a continuous basis. The effective date is 15 November 2024 and it is applicable across the financial services sector.

The standard requires the control functions and/or external assurance providers, to have the capacity to independently review and provide objective assurance of compliance with all IT-related activities as outlined in the financial institutions policies and procedures.

Joint Standard 1 of 2023 (IT Governance and Risk Management for Financial Institutions, 2023) covers the following:

Roles and responsibilities;

- IT strategy;
- IT risk management framework;
- Oversight of IT risk management;
- IT operations;
- Handling of sensitive or confidential information;
- Risks associated with financial products and financial services;
- IT programme and/or project management; and
- IT resilience and business continuity

The importance of IT governance

Some recent developments in the regulatory environment, once again emphasised the importance of governance and particularly IT Governance, as the foundation of an effective system of control on which technology can be built and used in a responsible and secure manner, for example the JSE CEO & FD attestation, UK SOX and now Joint standard 1. One should consider IT Governance as being the solid foundation on which your IT house is built – without the solid foundation, it doesn't matter what fancy technologies you build on top of it, ultimately it will come crashing down, hopefully not taking the organisation with it. If an organisation does not get the foundations of IT governance right, which addresses the fundamentals of IT risk, control, monitoring and remediation, how will you deal with the new and evolving topics related to or heavily dependent on IT, which include:

IT Governance is the life blood of a company and a solid IT Governance foundation is critical to provide a solid platform on which to build your digital landscape. The Board, together with Senior Management have the responsibility to ensure that the organisation has a robust IT risk management framework in place, which underpins the IT Strategy.

Melanie Miller

Partner
Tech Assurance
T: +27 82 717 0195
E: melanie.miller@kpmg.co.za

Key Actions

- Does the organisation have a formal IT risk management framework?
- How are you ensuring the consistency with which governance, risk mitigation and controls are applied at the entity and divisional level, but also supporting processes and third parties?
- Have IT risks been considered at divisional level and the IT risk management framework applied to address the unique risks relevant to the division?

7 Third party risk

7 Third party risk

The evolution of outsourcing

In today's interconnected world, reliance on outsourcing is increasing and they are engaging third party vendors in various capacities to enhance efficiency, reduce costs, and provide access to specialised expertise.

Outsourcing has become a global phenomenon, and South Africa is no exception. As financial institutions increasingly rely on external service providers, digitally transform, journey into the cloud, explore opportunities with artificial intelligence, they face unique challenges in the expanding reliance on third parties. As they expand on their products and service offerings through outsourcing, so do the challenges associated with managing outsourced risk.

Recent events such as the global pandemic, the geopolitical landscape and other factors has taught us not to undermine the importance of our interdependencies on key third parties as we have seen organisations and economies experience supply chain challenges, security incidents and data breaches. These will continue to grow and escalate in complexity. Whilst outsourcing is a key business enabler, so too is the effective management of the risks relating to outsourced services.

Emerging outsourcing risks

Some key risk dimensions with third-party relationships that include:

Financial Risks: These include the risk of financial instability or bankruptcy of a vendor, which could disrupt supply chains or contractual obligations. Further, commonly overlooked risk is a financial institution's potential risk exposure in the event of breaches / incidents / outages related to third party vendors, for example does the vendor have appropriate insurance or whether a financial institution's insurance extends to related activities for that entity that are executed by a vendor.

Regulatory Risks: : Third parties may impact your control environment through their operations, affecting your organisation's reputation and compliance. Where third parties are cross border, or not financial services providers, the potential for regulatory risk exposure to your financial institution is naturally increased. We have frequently heard the principle that you can outsource the service but not the accountability for the risk. This is affirmed in recent regulatory developments in the South African financial services sector which re-iterates management and the boards accountability for the risks, in an outsourcing arrangement. This is complicated by an evolving landscape and with changes expected to continue in this space, regulatory risks demand increased focus and on-going assessment of your regulatory risk exposures, not just locally but globally.

Reputational Risks: It goes without saying, but giving a third party access to your processes, customers or data inherently means that a third party's actions or misconduct can tarnish your brand image, leading to customer distrust and revenue loss.

Security Risks: Vendors often handle sensitive data, making them potential vectors for cyber attacks or data breaches. KPMG's Southern Africa CEO Outlook survey published in 2023, tells us that whilst 71% of CEO respondents believe that Gen AI is a top investment priority and are actively making investments in identifying opportunities related to Generative AI, 84% of respondents acknowledge that cyber security is a key risk.

We have seen instances of organisations exposed due to incidents that occur at third parties and this is a key focus for business leaders when embarking on new or continued relationships with third parties. Looking at this risk from a different angle, each third party you contract with represents a potential entry point for cyber threats. Weaknesses in the third party's security posture can be exploited and impact you. The more vendors you engage, the larger your attack surface.

Growing regulatory expectations

The regulatory landscape has seen a particular focus on outsourcing in the recent years, Regulators worldwide are focusing on third-party risk management frameworks and controls, and it's no different in South Africa. We have noted with interest the recent emphasis by regulators in ensuring robust risk management practices for outsourced services, with the release of Joint Standard 1, focused on IT governance. Our local FS regulators have over the past few years highlighted cyber risk and outsourced risk management as flavour of the years, which has indicated their focus. In the past few months, we have seen the following developments out of the FSCA and PA, that re-affirm the important focus by the regulators on outsourced risk:

- Issuance of Joint Standard 1 of 2023, titled Information Technology (IT) governance and risk management, which outlines the principles that financial institutions must adhere to in managing IT risk, with a specific emphasis on third party risk management, and guidelines for assessing and mitigating third party risks.
- Submission of a draft joint standard on outsourcing by insurers, that was submitted to Parliament and sets out guidelines / requirements for outsourcing that insurers must comply with, including outsourcing of material functions, outsourcing arrangements requiring regulatory notification and management and review of outsourcing arrangements, amongst others.
- Submission of a draft joint standard on cyber security and cyber resilience to Parliament

Challenges in managing risk

Whilst the battle to balance risk management with business outcomes becomes more prevalent in this evolving and complex landscape continues, it's clear that outsourcing is in place to derive efficiencies and this paradigm is increasingly being challenged.

In striving for the balance between innovation and risk mitigation in outsourcing strategies, some of the following challenges are often encountered:

- Responsibility and accountability – A key challenge in outsourcing is the lack of clarity between third parties and institutions regarding the distinction between responsibility for executing processes and accountability for outcomes.
- Assessing performance versus conformance – Often, service monitoring (evaluating performance against service levels) is confused with conformance. Whilst service level monitoring may provide management with comfort on the service, it may not always provide management with comfort that adequate processes and controls are implemented and operating at a service organisation. The use of certification and assurance reports like ISO and SOC reports are growing in prevalence, to respond to this. Further, we often encounter extensive due diligence activities that address conformance at the onboarding stage with a vendor, however the ongoing monitoring is critical to ensuring adequate management of your outsourced risk.
- Understanding assurance needs of stakeholders – In addressing the combined assurance needs of internal and external assurance providers, as relevant to key third parties, there is often a lack of understanding of the type of assurance being provided and its ability to meet the needs of assurance stakeholders. It is important for management to obtain an understanding of the differing certifications, assurance reports and other methods of demonstration of governance, implementation of policies, procedures and controls that third party service providers have in place or are considering obtaining and engaging with the respective assurance stakeholders to confirm that the relevant reports / certifications meet their requirements. This can be a source of much frustration, especially where certifications are obtained, but do not meet the needs of assurance stakeholders.

The governance of third parties by management is increasingly becoming a focus area as this risk landscape grows and its importance cannot be understated.

Why third party risk management

Against this backdrop, whilst Third-Party Risk Management ("TPRM") guidelines and frameworks exist, and have been around for a while, a renewed focus and transformation of TPRM programs are required, which clearly outlines the process of analysing, managing and minimizing risks linked to outsourcing, responds to some of the challenges highlighted above and is designed for an evolving technology and regulatory landscape. This would include more defined end to end life cycle activities for third party on-boarding, management and offboarding, increased focus on regular monitoring and conformance and possible leverage of automation and technology, to assist in third party risk management. The TPRM aims to strike a delicate balance: reaping the benefits of collaboration while safeguarding against potential threats.

In conclusion, as you consider the growth in prevalence of outsourcing, the opportunities that exist with outsourcing, the anticipated increased dependencies on third parties as organisations continue to embark on digital transformation programmes, exploring AI and ESG, and the dynamic and changing risk landscape, one thing is for certain, in an interconnected world, third-party reliance is inevitable. Financial institutions must proactively manage these relationships to minimize risks and ensure their businesses can thrive while safeguarding their interests.

Jatil Kassanjee

Partner
Tech Assurance
T: +27 82 716 8177
E: jatil.kassanjee@kpmg.co.za

Key Actions

In addition to the above, business leaders and boards need to consider emerging risk focus areas with a focus on AI and ESG:

- Are our third parties impacting the environment?
- Is AI being used to process our customers information and how do we know if decisions being made are ethical, free from bias and delivering the right outcomes?
- Is our proprietary and customer information safe and being used in a responsible manner?

8 Fraud and financial crime

8 Fraud and financial crime

Collaboration and cohesion to combat financial crime

Since the grey listing, the South African government has intensified its efforts to address the deficiencies that were identified in the FATF 2021 Mutual Evaluation Report. Part of these remedial efforts is to improve the legislative environment. This includes the amendment of six laws that are key to the effectiveness of South Africa's anti-money laundering ("AML") and combating terrorist financing ("CFT") measures.

The primary legislative change addressing financial crime in South Africa can been seen in the General Laws (Anti-Money laundering and Combating Terrorism Financing) Amendment Act 22 of 2022 ("GLAA") which was gazetted in December 2022. This Act amended several other Acts which govern the sphere of influence on commercial crime in South Africa, including the Companies Act; Trust Property Control Act; Non-Profit Organisations Act; Financial Intelligence Act and the Financial Sector Regulation Act.

Organisations therefore face significant pressure to enhance financial crime compliance frameworks in line with the regulatory framework. This includes adapting to evolving AML/CFT regulations, improving internal risk management and compliance monitoring practices, and actively participating in the regulatory change process. These efforts are crucial not only for maintaining regulatory compliance but also for safeguarding the integrity of the financial sector in South Africa.

To begin with, organisations need to have a deeper understanding of the evolving criminal threats and vulnerabilities. Only when an organisation understands the different schemes used by criminals to abuse the products and services offered, and the vulnerabilities when facing these threats, can effective measures be designed and implemented. This requires focusing on moving beyond compliance to being purpose driven and intelligence led.

Here are some essential pieces of advice for organisations looking to improve their financial crime risk management:

- **Strengthen Compliance Frameworks:** Ensure that your compliance frameworks are robust and align with the latest legal requirements. This includes understanding and implementing guidelines provided by the Financial Intelligence Centre Act ("FICA") and other relevant laws and regulations.
- **Implement Risk-Based Approaches:** Adopt a risk-based approach to AML/CFT (Anti-Money Laundering/Countering Financing of Terrorism) compliance. This involves identifying, assessing, and understanding the specific risks associated with different customers, products, services, and geographies.
- **Leverage Technology and Innovation:** Utilise advanced technological solutions such as Artificial Intelligence, machine learning, and data analytics to enhance your ability to detect and prevent financial crimes. These technologies can help in efficient transaction monitoring, customer due diligence, and identifying unusual patterns of behaviour.
- **Regular Training and Awareness:** Provide regular training to employees on AML/CFT regulations and the latest trends in financial crime. Ensuring that your staff is knowledgeable and vigilant is key to preventing financial crime.
- **Enhanced Due Diligence:** For high-risk customers or transactions, conduct enhanced due diligence. This should include a thorough investigation of the customer's background, business relationships, and the nature of their transactions.
- **Audit and Review Systems Regularly:** Regularly audit and review your AML/CFT systems and processes. This helps in identifying any gaps or weaknesses and ensures continuous improvement of your financial crime risk management strategies.
- **Collaboration and Information Sharing:** Collaborate with regulatory bodies, law enforcement, and other financial institutions. Sharing information can be critical in identifying and mitigating financial crime risks more effectively.

- **Tailoring Innovations to Operational Realities:** Integrating new innovations into a company's operational framework can be challenging. It requires a careful assessment of the company's existing processes, infrastructure, and culture. Customizing solutions to fit the specific needs and capacities of the company, while ensuring they comply with regulatory requirements, is crucial. It's also important to manage the change process effectively, ensuring staff are trained and the transition is smooth.

- **Consult Experts:** Given the complexities involved in financial crime risk management, consulting with legal and financial crime experts can provide valuable insights and help in effectively navigating this challenging landscape.

- **Monitoring and Reporting:** Establish efficient systems for monitoring transactions and reporting suspicious activities as required by law. Timely and accurate reporting is not just a regulatory requirement but also a crucial step in combating financial crime.

By following these guidelines, organisations can enhance their financial crime risk management practices effectively. Tailoring new innovations to a company's operational realities is challenging but essential for maintaining compliance and protecting the organisation from financial crimes. It requires a strategic approach, involving a thorough understanding of both the innovations and the organisation's unique operational context. Furthermore, perhaps the most significant action needed is the commitment of every stakeholder in this economy, both from the private and public sector, to work together, implement risk-based compliance and construct a trustworthy ecosystem in terms of AML/CFT. Collaboration and cohesion are key to the future progress of combating financial crime. The starting point of this partnership is trust and common purpose.

Candice Padayachee

Partner
Forensics
T: +27 82 718 8851
E: candice.padayachee@kpmg.co.za

Key Actions

- Make sure that your organisation has a practical understanding of the different schemes used by criminals to abuse the products and services you offer. Only when the vulnerabilities are understood can effective measures be designed and implemented.
- Implement a Risk-Based Approach which allows you to identify, assess and understand the risks associated with different customers, products, services, and geographies.
- Communicate and collaborate with the different regulatory bodies, law enforcement. Sharing information can be critical in identifying and mitigating financial crime risks more effectively.

9 ESG

9 ESG

Sustainability regulations outlook

2023 was the hottest year on record, and 2024 is forecasted to be even hotter. Climate-related extreme weather events such as droughts, floods, and heat waves are becoming more frequent and destructive and nature degradation and biodiversity loss is accelerating.

COP28 was held in Dubai from 30 November to 13 December 2023. As with previous conferences, there were several announcements with no substantive game-changing commitments. According to the Chair of the African Group of Negotiators on Climate Change, Africa had six priorities to be addressed going into the conference:

1. Just energy transition	4. Africa's quest to be granted special needs and circumstances status.
2. Strengthening adaptation Actions	5. Operationalisation of the Loss and Damage Fund
3. Climate Finance	6. Global stock take

Africa needs to be a part of the solution, not part of the problem

Africa represents 20% of the global population but only contributes 3% to global warming. The 2023 UN Sustainable Development Report states that of the 17 Sustainable Development Goals ("SDG"), Africa is on track to meet only one SDG by 2030: Access to the Internet and ICT. More than 600 million Africans lack access to energy and clean water. The world remains off track to achieve the Paris Agreement. The UN found that none of the 195 signatories to the Paris Agreement are currently on track to hit their National Determined Contribution ("NDC") targets.

Climate change exacerbates social challenges, with the poorest of nations and communities often the most affected, increasing existing inequality gaps. High levels of debt-to-GDP and high finance costs have significantly inhibited African countries' ability to respond to climate change. African and Middle Eastern leaders announced the formation of the Global Growth Green Institute ("GGGI") Safe Initiative worth $10 billion to address the food security challenge in Africa. The Multilateral Development Bank ("MDBs") said they will contribute $1.6 billion to support food systems that can handle climate change and create special zones for processing agricultural products.

Ten African countries joined the First-of-its-Kind Consortium to deploy 5 GW of battery Storage Systems. The AfDB proposed the creation of green banks and launched the Climate Action Window, which it will fund with USD 4 billion for seven low-income African countries by 2025. The AfDB also launched the Africa Climate Risk Insurance Facility for Adaptation ("ACRIFA"), offering $1 billion in loans.

The United Nations 2023 Global Climate Litigation Report show that people increasingly turn to the courts to combat the climate crisis and biodiversity loss. As of December 2022, 2,180 climate-related cases were filed in 65 jurisdictions. South Africa recorded nine cases; Nigeria, Kenya, and Uganda each recorded 2 cases; and the East African Court of Justice recorded one.

Global regulatory reporting developments

Central Banks and capital market regulators in Egypt, Ghana, Morocco, Nigeria, South Africa, Kenya, Tanzania, and Zimbabwe have been among the first African countries to make the 2017 TCFD regulations and disclosures mandatory. South African banks started with voluntary TCFD disclosures from 2019 onwards.

Various African countries' capital markets regulators, including Nigeria, Kenya, and Zimbabwe, have announced that they will also adopt the 2023 ISSB standards for listed entities. The 2023 ISSB standards have not yet been adopted as mandatory in South Africa. However, the country, through government, regulators, and business, are carefully considering the optimal pathway to adoption, including the value proposition for the country and cost vs benefit. In South Africa, the adoption question may not be if but when.

Going forward, financial regulators are expected to get tough on greenwashing. This year, the FSCA is expected to issue proposed product labelling regulations and associated potential fines to address local greenwashing under the Conduct of Financial Institutions Bill ("COFI"). The European Union ("EU") have drawn up plans to crack down on the practice of greenwashing. The plans would allow financial firms ten days to validate their green claims, otherwise incur substantial penalties.

The 2017 Task Force for Climate-related Financial Disclosures formed the base for the 2023 new proposed Basel Pillar 3 Climate Disclosure requirements, European Sustainability Reporting Standards ("ESRS") and International Sustainability Standards Board ("ISSB") IFRS S1 and S2 disclosure requirements. TCFD, TNFD, Basel, and ESRS global banking regulatory requirements are based on double materiality, while the ISSB reporting standards are based on single materiality.

Key sustainability regulatory developments

BCBS PILLAR 3 DISCLOSURES

On 29 November 2023, the Basel Committee for Banking Supervision ("BCBS") launched a consultation on a common baseline Pillar 3 disclosure framework for climate-related financial risks, with a comment deadline of 29 February 2024. The BCBS climate proposal requires more detailed disclosures than the JSE Climate Guidelines and IFRS S1 and S2 standards of the ISSB.

The committee proposes qualitative and quantitative changes to the current Pillar 3 disclosure rules, which lay out the public disclosures banks must make. It includes the disclosure of forward-looking transition information and the disclosure of three additional areas: Property Finance (commercial and retail), financed emissions and facilitated emissions from off-balance sheet activities.

BCBS will consider which elements would be mandatory and which are subject to national discretion. Basel is proposing an implementation date of 01 January 2025, one year after the effective date proposed by the ISSB and after the expiration of the ISSB's proposed transitional arrangements.

TASKFORCE FOR NATURE RELATED FINANCIAL DISCLOSURES ("TNFD") RISK FRAMEWORK

Around 85% of the world's companies depend significantly on nature, indicating the critical importance of greater transparency for market participants on nature-related risks and opportunities.

The TNFD risk framework offers a standardised approach for financial institutions to assess and disclose their impacts and dependencies on nature. The Banking Association of South Africa ("BASA") led the banking sector pilots, testing the TNFD beta-framework from June 2022 until February 2023. On 22 November 2022, BASA launched the South Africa TNFD Consultation Group and the final TNFD framework locally.

Equity Banking Group from Kenya and Ria Bronco Diamond Explorer from Angola committed to TNFD-aligned risk disclosures for 2024; KCB Banking Group and Icea Lion Insurance from Kenya, and Sanlam Insurance Group from South Africa committed to TNFD-aligned risk disclosures for 2025.

SUSTAINABLE FINANCE

The FSCA will continue working closely with National Treasury and the Prudential Authority to support the development of a sustainable finance market in South Africa as part of the Twin Peaks regulatory framework.

Conduct Of Financial Institutions Bill Sustainable Finance Implementation Plan

In preparation for the implementation of the COFI Bill, the FSCA has established various thematic workstreams to consider best practices regarding sustainable finance, to promote transparency, support the effective channelling of credit and savings for good, and reduce the risk of greenwashing, social-washing, and impact-washing.

The National Treasury Green Finance Taxonomy will form the basis for FSCA and South African Reserve Bank ("SARB") disclosure, reporting and assurance requirements. FSCA disclosure requirements will be set at both product and service levels. Assurance providers, including ESG rating agencies and ESG data providers, will be consulted during the drafting of disclosure requirements. The FSCA will issue a position paper clarifying its stance on International Standards.

COFI will also result in significant amendments to Regulation 28 of the Pension Funds Act, which deals with credential restrictions to pension funds and the infrastructure used to conduct services.

National Treasury will continue to drive the COFI Bill to entrench better ESG and customer outcomes in the financial services sector. As the adoption and enactment date of the COFI Bill draws closer, the Banking Association of South Africa and other banks need to work closely with the FSCA on developing the ESG conduct standards and what needs to be actioned based on the transitional arrangements expected to be finalised in 2025. During the first half of 2024, we expect a raft of proposals to be published for consultation.

CARBON CREDIT MARKETS

Carbon trading will likely become a significant factor this year as the National Treasury looks to tap into further tax sources and ESG targets increasingly tied up in corporate regulations. Last year, the Treasury and DFFE launched a consultation process to consider stakeholder inputs on the possibility of a domestic market to trade tax credits created through the carbon tax. The consultation will focus on "the building blocks needed to ensure seamless trading", the Treasury said in the 2023 budget that Finance Minister Enoch Godongwana tabled. The FSCA will support this process and prepare financial markets-related research and positions, particularly concerning a voluntary carbon market, as part of its Sustainable Finance Work Programme. The draft Carbon Framework is expected during the first half of 2024.

Current South African Carbon Regulations allow for when a company cannot reduce its carbon emissions to offset these emissions through credits for tax purposes. Last year, the Johannesburg Stock Exchange ("JSE") launched the JSE Ventures Carbon Market, allowing these voluntary carbon trades.

Ben April

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

Key Actions

On 14 November 2023 the ECB issued enforcement measures with potential fines to banks that lag on managing climate and environmental risks. Frank Elderson of the ECB stated "… at present none of the European banks under our supervision meet our expectations. We have started to adopt enforcement measures including the potential imposition of periodic penalty payments … if they don't comply, they will have to pay a penalty for every day the shortcoming remains unresolved."

The Sustainable Finance and ESG regulatory and compliance landscape is fast evolving and under significant scrutiny. We suggest that organisations:

- Perform independent TCFD compliance readiness and gap assessments across all significant subsidiaries and African jurisdictions.
- Capacitating risk departments in anticipation of the impending promulgation and implementation of the COFI Bill and its associated sustainability regulations for deposits, loans, bonds, and investments.
- Keep up-to-date with cross-border impacts of regulatory developments, particularly to countries with significant exposures.

10 Payments

10 Payments

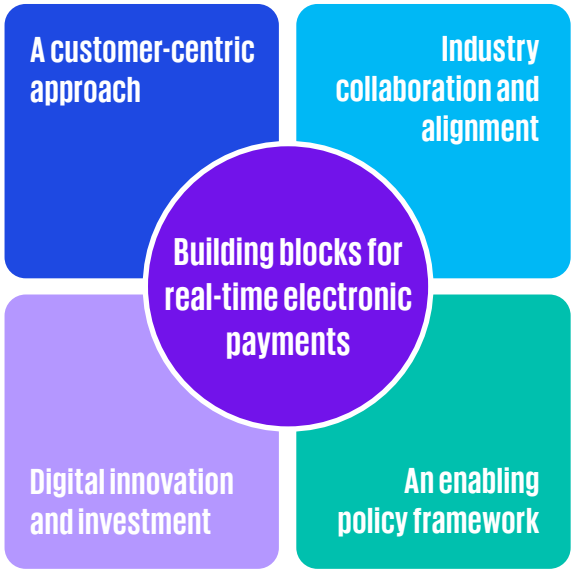
Building blocks for real-time electronic payments

Real-time (instant/immediate low-value credit-push) electronic payments such as PayShap and Transactions Cleared on an Immediate Basis ("TCIB") have the ability to significantly transform the domestic South African and regional crossborder ("SADC") payments landscape. Furthermore, real-time electronic payments can accelerate the nine industry goals of the National Payment System ("NPS") Vision 2025, which includes increased financial inclusion, enabling regional integration, and promoting competition and innovation, while maintaining the safety, efficiency, and accessibility of the NPS.

However, to truly unlock the full potential of real-time electronic payments and shape the future of payments domestically and regionally, there are four essential building blocks summarised below that can act as enablers.

The building blocks

- **A customer-centric approach:**- to remain sustainable, real-time electrotonic payments should continuously address the needs of consumers and businesses (e.g., the need for cost effective payments that clear and/or settle in real-time to improve liquidity).
- **Industry collaboration and alignment:**- the success of real-time payments can only be achieved through greater industry (banks and non-banks) collaboration and alignment.
- **Digital innovation and investment:**- digital innovation and investment across the NPS plays a pivotal role in shaping the future payments ecosystem, enhancing safety, efficiency, and fostering economic development.
- **An enabling policy framework:**- a clear and supportive policy framework that encourages competition and innovation while ensuring the safety and efficiency of the NPS provides a foundation for real-time payments innovation.



A customer centric approach

The customer-centric approach building block is about designing and implementing value-driven, real-time electronic payment solutions that prioritise the evolving needs of domestic and regional customers (e.g., lower-cost, real-time payment solutions). Currently in South Africa, an immediate domestic interbank payment ("IIP") person-to-person or person-to-business can cost a customer anywhere between ZAR45 – 60 per transaction, while a cross-border electronic payment can cost anywhere between ZAR150 to 750 per transaction with the traditional big banks. This is quite a costly endeavour to the end customer and proves a challenge for majority of the of the SADC people to access the formal financial system, considering other administrative costs associated with account maintenance activities.

The introduction of PayShap and establishment of non-bank remittance payment/ financial service providers such as Mukuru presents an opportunity for enabling the nine industry goals of the NPS Vision 2025, including financial inclusion, promoting competition and innovation, and cost-effectiveness. Educating the end customer on these developments will influence the extent of adoption and usage.

Industry collaboration and alignment

The transformative ability to leverage real-time payments to aid domestic and regional economic growth and accelerate financial inclusion requires industry collaboration that is aligned towards a common goal. The establishment of the new Payments Industry Body ("PIB") provides a stepping stone towards achieving NPS vision 2025 industry goals including interoperability, promoting competition and innovation, and financial inclusion. Moreover, paradigm shifts such as ISO 20022 and open finance architecture promote industry collaboration by providing common data formats, enabling interoperability, and enhancing transparency when adopting domestic and regional real-time payments innovation.

The need for industry collaboration is exacerbated by the FATF grey listing of SADC real-time gross settlement ("RTGS") member countries including South Africa, Mozambique, and Democratic Republic of Congo due to AML/CFT/PF deficiencies identified in the respective financial system(s). Therefore, a collective, transparent, and purposeful approach is essential to the sustainability of a safe, efficient, and accessible NPS.

Digital innovation and investment

Digital innovation and investment initiatives such as the renewal programme of the domestic and regional real-time gross settlement RTGS system operated by the SARB, introduction of PayShap, CBDC feasibility study undertaking by the SARB, and DebiCheck are crucial to enhancing integrity, efficiency, accessibility, and sustainability of the NPS. Moreover, these initiatives represent a collective industry effort to support the realisation of the nine industry goals of the NPS Vision 2025 such as cost-effectiveness, interoperability, and promoting competition and innovation.

Issues such as different maturity levels of data and cyber laws across SADC countries and a worrying recent trend in South Africa where victims are kidnapped or hijacked and violently forced to make immediate payments from their banking digital channels to accounts or channels accessible to the criminals, negatively impact the adoption and usage of digital payment innovations. To address these issues, the payments industry needs to consider interoperability at the forefront of digital innovation enabled by paradigm shifts such as ISO 20022.

An enabling policy framework

An enabling policy framework is a fundamental building block that is required to facilitate the transformative adoption of real-time electronic payments, helping shape an accessible, inclusive, and innovative domestic and regional payment landscape. In essence, an enabling policy framework needs to be characterised by agility and adaptability to give effect to real-time payments that have the ability to efficiently and effectively enable trade and remittance across the SADC region.

Ongoing domestic policy changes such as the consequential amendments to the NPS Act seek to empower the inclusion of eligible non-bank participants (e.g., telcos, retail, big tech, fintechs) into the domestic and/or regional settlement system(s). Furthermore, giving recognition to new forms of payment instruments such as tokenised instruments that can help optimise real-time payments and lead to more digital enabled payment innovations.

Ultimately a dynamic and adaptive policy framework is core to fully realise the potential of real-time electronic payments as a catalyst for domestic and regional economic growth and financial inclusion.

Sydney Khumalo

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

https://techcentral.co.za/banking-app-kidnappings-south-africa/234770/

Key Actions

- Build interoperable payment infrastructure and systems to help accelerate digital enabled payment innovation.
- Prioritise the strengthening of security measures to protect customer transactions and data, while ensuring compliance with domestic and/or regional AML/CFT/PF and fraud regulations.
- Develop a customer centric approach that promotes the principles of financial inclusion.