KPMG

Ten key regulatory challenges of 2019

Resiliency amidst innovation

2019

Kpmg.co.za

Contents

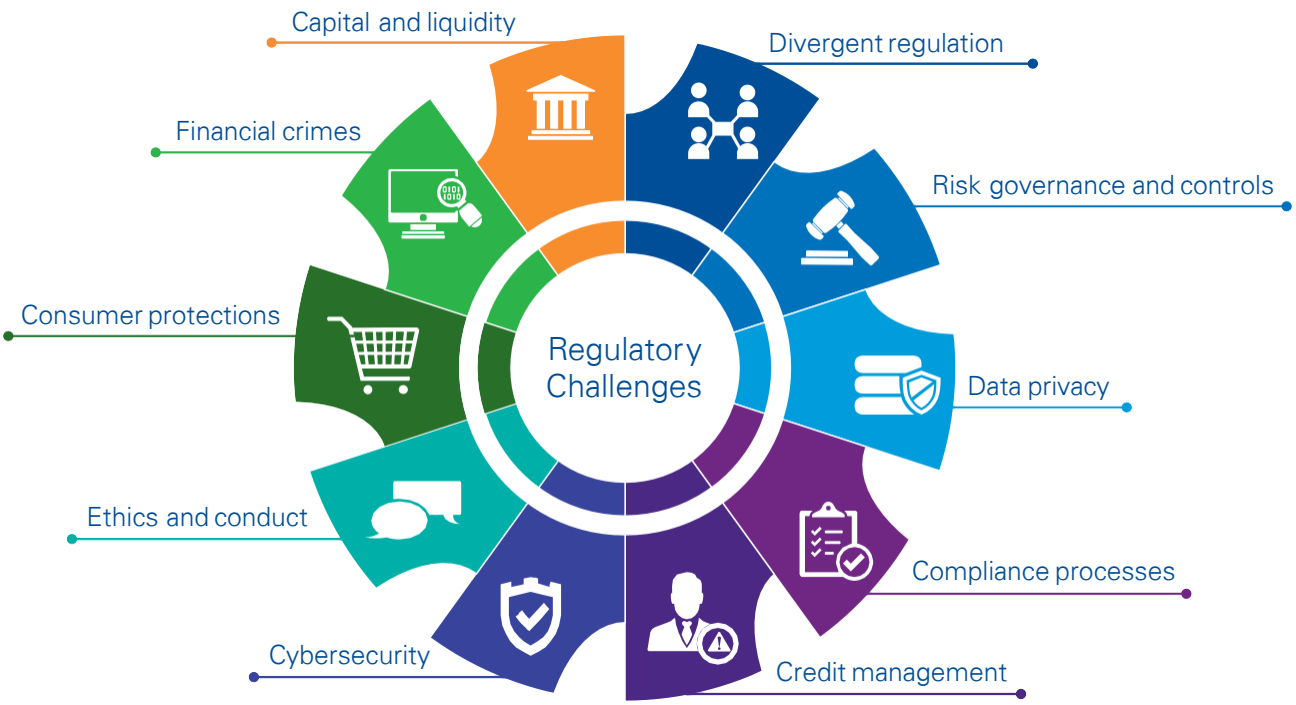
Introduction

The financial services industry is experiencing dramatic transformation, challenging both regulators and traditional financial services firms to keep pace.

Fueled by rapid emerging technologies, global interconnectedness, changing economic and jurisdictional factors, competition and consumer demand, firms are innovating—embracing new business models and adopting automation to support their operations and regulatory obligations. As firms pursue greater agility and resiliency, they are expanding their use of advanced data analytics, artificial intelligence, and innovative technologies, triggering further risk governance adjustments and regulatory attention in areas including safety and soundness and consumer protection.

In 2019 and beyond, regulators will assess how firms are adapting to market pressures and managing the associated risks, focusing on firms' operational resilience, governance and controls, data security, and consumer protection—and expecting all to align with ethical and sound conduct practices.

KPMG highlights the key drivers and actions for firms in the following Key Ten Regulatory Challenges for 2019:



An evolving regulatory landscape

Drivers

- New financial services legislation and regulation
- Global divergence in regulation
- Growing awareness of reputational and strategic risk
- Regulatory focus on improved risk and capital management practices
- Drive for capital optimisation

Challenges

The Financial Services Regulation (FSR) Act was signed into law in August 2017, and fundamentally changes the regulatory architecture of the financial services landscape in South Africa. The FSR Act gives effect to the Twin Peaks model of regulation, effectively establishing the Prudential Authority with a mandate to maintain and enhance financial stability and the Financial Services Conduct Authority, responsible for supervising the conduct of financial institutions.

Regulatory activity will be driven via:

- **State enacted laws and promulgated regulations.**
  - The Prudential Authority implemented the Solvency Assessment and Management (SAM) regulatory regime, effective 1 July 2018, through the promulgation of the Insurance Act of 2017. This will, for most insurers, mean a marked shift in regulatory capital requirements.
    The introduction of SAM also crystallises requirements for own risk and solvency assessment (ORSA) requirements as well as the development and implementation of a Capital Management Policy.
    Furthermore, the Prudential Authority is expected to introduce in 2019, new auditing requirements for the annual statutory submissions to the Regulator.
  - Many insurers will look to optimise their capital levels and structure in 2019 to improve shareholder value.
  - New audit requirements of the annual statutory returns, will challenge not only insurers who need to make sure that the relevant figures and underpinning calculation kernels are such that they may be efficiently audited. Auditors will need to appropriately change their audit process and approach to ensure full coverage of expected audit sign-off of the statutory returns.
  - Most insurers will have to develop a formal capital management policy with a few looking to refine the existing policy and align it with the capital management process, wider risk management framework, Head of Actuarial function responsibilities and board-approved risk appetite statements.
  - Many life insurers have developed or are considering developing liquidity metrics for the business and setting appropriate liquidity related risk appetite statements.

KPMG

An evolving regulatory landscape

As part of the transitional arrangements to full implementation of the FSR Act, the Prudential Authority will require insurers to convert the existing insurance licence to a licence under the Insurance Act. All insurers will have to undergo this process in the next two years. This process will be initiated by the Prudential Authority.

— **The draft Conduct of Financial Institutions Bill** was published in December 2018 and is open for public comments until April of 2019. This Bill moves away from institutional to activity based regulation. It is principles and outcomes focused, risk based and proportionate, which will allow the regulator to monitor and enforce the achievement of positive outcomes.

— **Nonbank supervision**
- Evolving regulatory coverage and standards are of key importance in areas of high innovation such as artificial intelligence.
- The Reserve Bank has called for commentary on its phased approach to the regulation of crypto currencies (which do not have similar safety mechanisms as the rest of the financial system)

— **Jurisdictional policies**
- These include sanctions and tariffs which trigger the potential for retaliation not only to countries by global service providers and to a globally connected market. Such policies often force changes to business strategies, staffing and capital allocations. Other jurisdictional events, such as the UK's Brexit, necessitates similar reassessment.

KPMG

Key actions

- Integrate regulatory inventory and rule mapping to operational controls.
- Identify interdependencies in business, product, and vendor process and controls for potential jurisdictional risks.
- Assess strategic, operational, and reputational impacts of emerging financial and non financial risks.
- Retool risk assessments, as appropriate.
- Formalise incident and issues management governance, processes, escalation, and reporting.
- Reassess capital and human resource strategies and allocation.
- Evaluate tax implications to changing regulatory policies.
- Complete change impact assessments.

Principles for the development of regulatory frameworks for financial markets

National Treasury seeks to develop harmonised and equivalent regulatory frameworks to ensure South African market players can continue to trade across borders. South Africa's regulatory and supervisory framework must be assessed as equivalent by regulators in other jurisdictions to ensure a level playing field, minimise duplication and uncertainty, and reduce the opportunity for regulatory arbitrage.

Source: 2018 Financial Markets Review, issued by National Treasury

Risk governance and controls

Drivers

- Heightened regulatory standards and expectations for the strong risk management practices
- Examiner focus on conduct, reputational, and strategic risks
- Agile business adoption of new technologies, new products, and new market entrants (e.g. fintech, regtech)
- Cost containment initiatives driving risk convergence and transformational initiatives
- Continuing market and consumer/demographic shifts
- Third-party providers, aggregator, and partner risks

Challenges

Financial service providers must maintain governance and controls within their risk management frameworks for sustainability, resiliency, and efficiency.

Key areas of focus include:

- **Strengthening of risk management practices**
  Examiners expect firms to strengthen oversight and assign specific accountability for the management of risks facing the firm, including enterprise risk identification, risk assessment, scenario analyses, issues management, controls, and reporting capabilities. Examiners assess how well operational controls enable appropriate risk management practices in practice.
- **Third-party risk management**
  Third parties, aggregators, and partners can present significant reputational risks to firms, even when acting seemingly independently from the financial institution (e.g. fraud, sanctions, human trafficking). Furthermore, regulators are concerned about firms' abilities to manage and mitigate their exposures from third parties (e.g. compliance failures, cybersecurity weaknesses, data privacy breaches). Proper risk management must be supported through controls, initial and ongoing, due diligence, risk assessments, monitoring, and auditing of third-party relationships, proper staffing allocations—and governance.
- **Risk governance**
  Risk governance (inclusive of risk committees) is central to helping assess risks. Firms must demonstrate an ability to effectively measure and mitigate risks but also anticipate and prevent risks, demonstrate resiliency and an ability to timeously adapt to market shifts. Regulatory guidance reconfirms the role of the Board of Directors and management in the risk governance structure.
- **Change management**
  Change management capabilities must support firms as they pivot business models, delivery models, automation, and reliance on third parties, among others shifts. Critical change management efforts across people, processes, and technology are critical to successful risk awareness and mitigation execution.
- **Information technology and data governance**
  Technology is elevating firms' ability to aggregate data (structured and unstructured) in real time and providing a deeper appreciation of risks enterprise-wide, including through dashboard visualisation capabilities. Regulatory expectations for model risk validations of technology systems, data governance, and for the validation and reporting of data for regulatory purposes are growing.

KPMG

Key actions

— Determine if operational controls, particularly for high-risk regulatory requirements, are functioning effectively.

— Engage with stakeholders to evaluate ways to enhance agility in risk management.

— Build change management components/steps into project plans.

— Identify processes or controls to converge in support of a stronger risk management approach enterprise-wide.

— Revisit data governance programs and protocols and refine them as necessary to meet regulatory scrutiny and to prepare for future automation efforts.

— Further integrate third-party risk management efforts across performance-based areas, jurisdictions, risk functions, and disciplines for improved governance and oversight.

Data privacy

Drivers

— Heightened public awareness of the value of and risks to consumers' personal data

— High-profile, widescale, publicised breaches

— Heightened expectations regarding the breadth of consumer information to be protected and consumers' rights to control use of their data

— Highly interconnected financial systems with multiple entry points

— Complexity of legal and regulatory landscape

Challenges

The heightened focus on privacy as a fundamental consumer right and the global spotlight on the European Union's General Data Protection Regulation ("GDPR") have put a spotlight on the protection of personal information in the South African context. This is despite the fact that the Protection of Personal Information Act of 2013 ("POPIA") still awaits an effective date for the provisions which require compliance from the entities processing personal information.

The South African Information Regulator has officially occupied office since 1 December 2016. Notwithstanding that the substantive provisions of POPIA are not yet effective, the Information Regulator has informally been handling various complaints received from consumers and has been engaging with companies who have been the subject of material information security breaches during the course of the previous year. As part of this engagement, the Information Regulator has convened meetings with various government institutions, including the HAWKS, the National Prosecuting Authority, the National Credit Regulator and the Association of Credit Bureaus and other foreign data protection authorities, such as the United Kingdom's Information Commissioner Office.

A level of uncertainty remains insofar as the extent to which companies should already be implementing the requirements of POPIA from a consumer relations perspective, with certain service providers to financial institutions refusing to take any tangible steps towards compliance until an effective date for POPIA is announced. This places organisations in an unenviable position in balancing the longstanding relationships they may have with their key service providers with the need to provide a customer-centric service offering to their clients.

Despite this uncertainty, the financial services market appears to be leading the front insofar as identifying and mitigating challenges in the context of local and international data protection regulation. We set out below some of the key challenges which have emerged within the South African privacy / data protection landscape:

— **Consent management**

Consent is but one of the lawful justifications for processing of personal information. However, relying on consent as a justification for processing personal information potentially creates an additional administrative burden under both POPIA (and the GDPR). This is due to the specific requirement for consent under POPIA (and the GDPR) - that is, that it cannot be implied and must be voluntary, specific and informed. In order to meet this requirement, any notice which an organisation uses to inform its data subjects of the nature and purpose of processing personal information must be sufficiently specific for data

Data privacy cont.

Drivers

- Heightened public awareness of the value of and risks to consumers' personal data
- High-profile, widescale, publicized breaches
- Heightened expectations regarding the breadth of consumer information to be protected and consumers' rights to control use of their data
- Highly interconnected financial systems with multiple entry points
- Complexity of legal and regulatory landscape

subjects to be in a position to provide such informed consent.

As data subjects may withdraw their consent at any time (subject to the provisions of section 11(2)(b) of POPIA), there is a need for organisations to put in place a process which enables them to manage consents and withdrawals of consent and respond accordingly.

— **Data subject requests**

While data security remains top of mind in the context of data protection and privacy, the management of personal information insofar as access requests, deletion and portability are concerned is a significant challenge for financial services firms. On 14 December 2018, the South African Information Regulator published the relevant forms to be used when a data subject wishes to request a correction or deletion of personal information in terms of POPIA. Few South African companies, however, have established formal processes through which such requests may be received and actioned across the organisation and the systems it uses.

— **Management of third party vendors**

The use of third party service providers to process personal information, such a tracing agents, credit bureaus, forensic investigation services and other service providers, are a potential areas of risk. POPIA requires that all responsible parties (organisations which determine the purpose and means of processing personal information) ensure, through a written contract that its third party "operators" (persons who process person information for an on behalf of the responsible party) establish and maintain the relevant security measures referred to in POPIA.

Beyond the contractual requirement which POPIA imposes on responsible parties, the extent to which financial service companies should have insight into their third party "operators'" specific security measures and be involved in the monitoring of their compliance, will need to be considered in the context of the nature and volume of personal information being processed by the "operator" concerned. Additional monitoring processes will further add to the financial services firms' administrative burden, but will be necessary in order to manage its risk exposure and protect the rights of its customers.

— **Reporting obligations under the Cybercrimes Bill**

Related to information security and privacy, financial institutions will need to be aware of the obligations which are sought to be placed on them under the current version of the Cybercrimes Bill. The Cybercrimes Bill seeks, amongst other things, to impose obligations on electronic communications service providers and financial institutions to report cybercrimes and provide technical and other assistance to the police in their investigation of cybercrime. The Select Committee on Security and Justice (within the National Council of Provinces Committee ("NCOP")) has called for written comments on the Cybercrimes Bill to be submitted by 8 March 2019 in anticipation of NCOP Security and Justice Committee hearings.

KPMG

The imminent changes to the South African consumer protection landscape will require organisations to develop a thorough understanding of their privacy and data security risk assessments and the existing controls in place to mitigate against those risks (whether internal or external to the firm) and to identify those areas where additional efforts are required to strengthen the effectiveness of their programs. This is necessary, both for the sake of managing the legislative risk involved and cultivating customer trust in this industry.

Key actions

- Inventory all personal information collected, processed, disseminated, stored and destroyed. Identify which personal information is "critical" to the organisation.
- Identify the purpose and the organisation's justification for processing personal information. Where consent is being relied upon, ensure that the notice against which consent is to be given is sufficiently clear and specific as to the purpose for collecting and processing the personal information.
- Develop, implement and maintain policies and processes which enable the organisation to:
  - Receive and manage consents and withdrawals of consent;
  - Respond to withdrawals of consent, which may include the cessation of processing unless there is other legislation which provides for such processing;
  - Receive and manage data subject requests;
  - Effectively manage its risk exposure to third party "operators" through the monitoring their compliance with the relevant security safeguards require under POPIA, where appropriate;
  - Monitor and report on security breaches and cybercrimes as required under POPIA and the Cybercrimes Bill respectively.

According to a KPMG survey of nearly 7000 individuals globally, nearly 75% of respondents have low levels of trust in insurance organisations that process their personal data, with just 7.7% indicating that they trust insurers completely. This is in stark contrast when compared to banks, with 40% respondents indicating that they have high levels of trust in respect of the banks processing their personal data. These statistics should raise alarms with senior executives across the insurance sector as in the absence of trust, customers are likely to be increasingly resistant to share their personal information, potentially undermining future insurance business models and strategies.

Source: KPMG Global Privacy Advisory practice, as published in The London Journal 2018

Compliance processes

Drivers

— Increased market competition and pressure to cut operating costs

— Expanded role of ethics and compliance, requiring greater diversification of skill sets

— Regulatory expectations of stronger compliance management in the first line

— Expectations by leadership for more "real time" compliance risk management, including upon trigger events, and consistent view of compliance risks enterprise-wide

— Extent and pace of change in both laws and regulations and regulatory bodies

Challenges

Firms are focused on bridging business and compliance objectives while avoiding regulatory, compliance, and ethical risks. At the same time, compliance leaders face an expanded mandate that increasingly includes culture/conduct, data privacy, and financial crimes among other regulatory obligations, a cost cutting corporate environment and regulatory priorities that include compliance and operational resiliency. Yet, advances in artificial intelligence and automation present opportunities to incorporate digital transformation to meet their challenges—operationalising compliance within first line processes and controls, while simultaneously enabling organisations to respond with greater agility to shifts in consumer behaviour and a tight employment market. To take advantage of such technology, firms must first reassess their core processes and controls to determine where more streamlined governance and enhanced risk management might add the most value.

In particular, firms should look at:

— **Increased governance expectations**

The IMF in its article IV report consultation (2018) with South Africa welcomed ongoing initiatives to further strengthen financial sector stability, including the new Financial Sector Regulation Act. However, several impediments to growth were highlighted including inter alia policy uncertainty, regulatory overreach and corruption. In this context firms must actively manage the flow of information to the board to keep it properly informed of aggregate compliance risks and to enable the board to provide clear, aligned, and consistent direction on the firm's strategy and risk tolerance.

— **Converging compliance risks and controls**

To further drive consistency in managing ethics, compliance, and reputational risks, firms are further converging their risks and controls across operational and business units and also across governance, risk, and compliance levels, enabling leadership to gain one consistent view of enterprise-wide risks, and pinpointing areas of highest risk. In addition, as regulators look to assess the strength of compliance risk-management practices, convergence and further operationalisation of compliance controls orient employees to the firm's risk strategy and highlight risk outliers with greater specificity.

— **Regulatory changes**

Given the plethora of changes in laws and regulations and the varied rate at which they occur, change management has become an organisation-wide imperative. Failure to properly and timeously implement changes could result in compliance and reputational risk as well as statutory damages and civil liabilities in some cases. Other factors, such as complex regulatory structures and uncertainty, merger and acquisition activity, new entrants, products and services, and talent constraints, are further challenging firm's efforts to update supporting operating systems and manage existing compliance management systems. In response, firms can map their regulatory obligations and risks to the appropriate functional level of business controls, facilitating a quicker impact analysis, strategic plan, and implementation of changes.

KPMG

— **Consolidating testing, surveillance and investigations**
Firms need to further integrate and coordinate across disparate compliance activities inclusive of testing, surveillance, and investigations, and deploy data analytics and metrics that are multidimensional across these for a more comprehensive understanding of compliance risks and pockets where gaps exist. It is important that data is not duplicated for an accurate perspective of where risk is pervasive, to assess the materiality of risks and to evaluate trends, root causes and systemic issues for further addressing. Automation and integration can break down silos and consequently drive positive cultural and ethical changes, in a more cost efficient way.

Firms face additional compliance challenges from:

— **New regulatory regime**
A new era for financial market regulation in South Africa has commenced with the twin peaks model of a Financial Sector Conduct Authority (FSCA) overseeing market conduct and the Prudential Authority (PA) taking responsibility for prudential regulation. The Financial Sector Regulation Act mandates co- operation and collaboration between authorities and the required Memoranda of Understanding (MOU) between the SARB, PA, NCR and FSCA will support such aim. In addition, the draft Conduct of Financial Institutions (COFI) Bill 2018 will further strengthen how the financial service industry treats its customers.

These developments will place increasing demands on compliance leaders and teams to apply broader perspectives and more sophisticated methodology and tools.

— **Attention to records/data retention and security**
The advent of GDPR and POPI have necessitated firms addressing increased arrangements over data governance and privacy. These obligations are exacerbated by the extent of cybercrime which, according to SABRIC's Digital Banking Crime Statistics, have more than half of them taking place online. The Prudential Authority published guidance for the Regulation 39 of the regulations relating to banks requiring appropriate governance, including the risks arising from use of cloud computing and offshoring of data. Firms will have to address these risks and compliance requirements.

— **Third-party relationships**
Third-party relationships can present reputational or financial risk to the firm, particularly when they engage in fraud or misconduct.

— **Charismatic leaders**
Charismatic leaders can be a hinderance if they do not allow for effective challenges and/or they restrict the flow of information and data about risks.

Key actions

— Refine compliance metrics and data analytics to provide more valuable, and consistent, risk information to the board.

— Identify opportunities to converge controls across the three lines of defence for more streamlined compliance, improved risk management, and enhanced first-line ownership of compliance risks.

— Evaluate regulatory change management processes in place, including agility and resiliency of those processes.

— Determine where silos between discrete compliance activities can be further broken down for a more integrated compliance risk management approach, and enhanced effectiveness.

— Develop a plan to achieve more "real-time" compliance based upon compliance risks, data availability, and integrity.

Top compliance automation challenges

In a 2018 survey of leading US based industries, more than 50% of CIO's and CCO's surveyed are not yet automating their compliance activities. 90% plan to increase automation funding in the next several years. Only 1in 5 has a well-defined enterprise wide strategy to automate compliance. Compliance automation is challenged by:

Misunderstood and/or insufficiently managed dependencies	39%
Leadership and/or stakeholder attention	36%
Insufficient metrics for measuring progress	35%
Unavailable resources	32%
Unavailable data or data did not have the anticipated integrity	26%

Source: KPMG Compliance Automation Survey 2018

Credit management

Drivers

- Economic shifts and increasing interest rates
- Changes to accounting standards and regulatory requirements
- Heightened regulatory concern for trends in leveraged lending and securitisation
- Identified supervisory priority for banking organisations

Challenges

Through 2019 banking and financial services organisations will face increased credit risk challenges with the embedding of the IFRS 9 concepts and the upcoming Basel 4 changes, the majority of the issues faced will be due to the shift in impairment methodology relating to IFRS9.

Key areas of focus include:

- **Commercial and retail underwriting**

  IFRS9 has caused banks to change their view of impairments. The change in concept from incurred losses under IAS 39 to expected credit losses required by IFRS 9 requires banks to raise impairment from day 1 for new exposures. Added to this, the forward looking component and requirement to recognise lifetime expected credit losses and the costs around loans have increased. In Southern Africa the books are already risky, which may cause banks to look for different avenues to increase their exposures and reduce their impairment cost. This may be in the form of limiting overdrafts to existing customers or a change in the current structure of products. Specifically in terms of the pricing and tenor.

- **Credit Risk Management**

  Going forward IFRS 9 requires banks to delay the write-off of non-performing loans to the point where further recoveries are unlikely. The change in the write- off point for non-performing loans could result in banks holding NPLs on the books for longer. The recognition of lifetime expected credit losses due to significant credit deterioration is expected to drive increased volatility in impairments over the course of the credit cycle.

The major change to daily operations is the greater amount of input required from the risk management teams when determining impairment. The greater reliance on risk information in terms of forward looking risk estimates and change in risk assessments will require increased integration of the risk and finance data environments, due to the forced integration between the Finance and Credit functions. The role of the Chief Risk Officer is expected to increase with the roll-out of IFRS 9, given the responsibility for the risk inputs used to calculate IFRS 9 ECLs.

Other areas impacted by the roll-out of IFRS 9 are:

- The need for management to better understand the budgeting and forecasting impact of IFRS9 and what it will do to their impairments.
- The complexity introduced into the operating environment and the reliance on internal models, which is contrary to the trends observed for baking regulations, where regulators have been moving towards more simplified approaches on the capital (Basel) side.
- IFRS9 has also caused a shift in Board responsibilities. The Board now needs to understand credit risk,

impairments and the accounting implications. For smaller banks, relationship board members will now need to skill-up.

— **Internal controls**

Credit risk standards were written for sophisticated banks with proper data management. The standards assumed that all the required data for IFRS9 was already set up. This has, however, not been the case throughout the majority of Africa. Even in places where historical data was saved, it often excluded important IFRS9 data such as the probability of default at inception. BCBS239 and the Risk and Data Aggregation and Risk Reporting (RDARR) requirements for banks are onerous and for those still struggling to implement basic risk models, let alone IFRS9, this is an added burden. On the South African side, the majority of banks have the data and infrastructure in place for IFRS9, but through the rest of Africa, this has been a problem.

— **Market view**

One of the guiding principles of IFRS and Basel was that the standardisation would increase transparency and comparability of Banks. IFRS9 though, seems to be doing the opposite. Many of the inputs into the impairment calculation rely on judgement and the internal economic view of the bank, modelling and data assumptions. IFRS9 has many moving parts including data assumptions, segmentation assumptions, the internal view of Significant Increase in Credit Risk (SICR) and data periods. These are all subject to the bank's judgement. Add to this, the forward looking view of banks, and you have a case where there are very different views across different banks, which further increases the comparability difficulties.

Key impacts to consider

— IFRS9 is increasing costs. Will consumers need to pay more for credit?
— Banks will have further complexities to manage.
— Credit data aggregation and reporting will be more complex, especially through Africa.
— As IFRS9 increased the use of judgement, comparing banks in terms of impairments becomes more difficult. How then do we interpret a bank's judgement?

Commercial and retail credit loan underwriting, concentration risk management, credit risk management, and the allowance for loan and lease losses, including preparation for CECL, are collectively one of the five supervisory priorities.

Source: OCC Fiscal Year 2019 Bank Supervision Operating Plan

Cybersecurity

Drivers

- Evolving and increasingly sophisticated technologies introducing new threat vectors
- Regulatory and consumer expectation for data protection, breach notification, and remediation
- Regulatory focus on operational resiliency
- Interconnected systems with multiple entry points
- Varying objectives for cyberattacks, including theft, destruction, and disruption

Challenges

Cyber attacks against financial services firms and other sectors have increased in number, size and sophistication. Globally, cybercriminals have siphoned billions of dollars from bank accounts as well as stealing millions of credit card records, by engaging and launching large-scale attacks against banks and other financial institutions. The financial services sector is a prime target for cybercriminals because of the tremendous value of information they hold. As attacks increase and regulators take more notice, the pressure for financial institutions to act is mounting.

Multiple forces are currently at work:

- **Cybersecurity is an increasing concern for organisations especially governments,** with the rise and investment in technology striving to provide universal access to the Internet. South Africa is quite a distance behind advanced economies in cybersecurity legislation, in government direction, in engagement with business and citizens, and in the supply of skilled labour. The delays that have been incurred has resulted in South Africa lacking in experience that is obtained in faster moving countries, and the improvements they have made to their policies and, especially, implementation.
- **Cybercrime a matter of national** security, with the world becoming increasingly digitised, it's no longer unthinkable that a cyberattack could shut down an entire electricity grid or even the water supply to a town or municipality. South Africa's Defence Minister, Nosiviwe Mapisa-Nqakula recently said the country is paying attention to cybercrime "at the highest level". With the pending implementation of the Cybercrimes and Cybersecurity Bill, expect cybersecurity to be a key policy issue in 2019.
- **South African Reserve Bank has released Guidance Note G4/2017,** most in regards to acknowledging the current importance of cyber resilience in regards to the rise of the relevance of cyber resilience for the financial market infrastructure (FMIs). This guidance was put together by the Committee on Payments and Market Infrastructure (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO).
- **Operational resiliency is a horizontal theme for 2019.** Considerations are that review will include a firm's key markets and products, having key systems in place to support the business, and the security and resiliency in those systems against breach and/or failure. Firms will be expected to understand what a system or operational failure will imply for the firm, its counterparties, and the economy overall, and they should be to demonstrate solutions and controls to reasonably detect and mitigate cyber threats, including an ability to ring fence critical

KPMG

aspects of their program such as the security of systems access. Firms may be challenged to closely align cybersecurity risk management with their business and growth strategies.

— **The growing sophistication of cyber attacks** and the speed at which technologies are evolving can make it difficult for firms to keep up, increasing the risk of unauthorised access to operations and systems, and amplifying the risk of fraud, reputational damage, and an unavailability of key assets. Regularly maintaining and increasing the levels of preparedness is critically important to cyber defences. Financial services firms have been challenged by:

  – Establishing cyber risk governance, including board oversight;

  – Recruiting and retaining specialised talent, and training existing personnel to identify and report suspicious activity;

  – Investing in new technologies, upgrading legacy systems, and integrating systems;

  – Meeting incident response, notification, and disclosure requirements/expectations;

  – Managing third-party data security and privacy risk.

Key actions

— Conduct cyber threat simulations to test controls and incidence response

— Evaluate cyber risk landscape and establish risk appetite alignment to drive effective mitigation prioritisation

— Develop and implement a forward-looking comprehensive cybersecurity strategy based on this with flexibility to accommodate change (internal and external) and addressing:

  – Identification of the relevant laws, regulations, certifications and standards

  – Organisation and governance, including board oversight, leadership accountability, and reporting, and data science talent

  – Policies, procedures, and controls, including authentication and encryption protocols

  – Internal and external risk assessment and management

  – Integration with existing solutions and processes

  – Ongoing monitoring and testing, alert thresholds and triggers, trends analysis

  – Ongoing security and risk assessments, disclosures and remediation, including identification of responsible/ incidence response, notification and reporting requirements and accountable personnel

  – Resilience and recovery measures for critical systems and data along with business continuity planning

— Design and layer multiple protective solutions to detect, prevent, and deter fraud.

Ethics and conduct

Drivers

- Social media mobilisation based on incidents of questionable or unfair treatment.
- Innovation and disruption by app-driven and behavioural competitors better able to promote and reward positive customer outcomes, for instance saving
- Continued supervisory focus on the abilities of firms to effectively monitor and manage misconduct by employees, third parties, and partners/ affiliates
- High profile regulatory enforcement actions and high value civil money penalties involving sales practices abuses, client suitability, and misconduct
- Increased awareness on nonfinancial risks, including reputational, strategic, and fraud risks, which can be tied to misconduct

Challenges

Over the last couple of years, the regulatory focus in financial services in South Africa has been trained on market conduct, fair treatment and the protection of customers. The focus led to the introduction of the twin peaks regime including the introduction of the Financial Sector Conduct Authority. Ironically, it was the general public that took up the baton last year when the insurance industry's repudiation practices were robustly challenged. Between the regulator and the public, firms will be forced to venture beyond law or industry norms to seriously consider the common wisdoms, habits and practices of the industry.

Areas of focus include: financial inclusion and responsible lending practices; suitability of products sold to consumers; sales practices and vulnerable consumer groups; fee structures; understandable and responsible financial advice; appropriate incentives; and consumer data privacy.

Challenges to managing conduct risk include:

- **A broad definition**

  Conduct risk seems easy enough to understand. It focuses on the ways in which a financial institution (and persons acting on its behalf) can exploit or unfairly treat customers and thereby negatively impact market stability. As soon as one tries to manage conduct risk, however, problems of definition arise. If one defines conduct risk too broadly, it encompasses too much (and a conduct risk register would become encyclopaedic in size); if one defines it too narrowly, one risks missing the point of conduct regulation, moving towards detailed rules rather than values and principles.

- **Positioning conduct**

  Given the broad scope of a term like "conduct", it is not immediately clear who should take responsibility for it. Conduct matters fall within the ambit of the ethics office, risk management, compliance, human capital and legal. Some banks solve the problem by designating a conduct officer, but then still face the challenge of efficient collaboration and clear mandates.

- **Who decides what's fair?**

  While a new regulation (and in this case, a new regulator) often sparks a focus on what "the regulator" expects, with conduct and treating customers fairly, it might not be that simple. The power of social media mobilisation highlights the need to ask more than "What does the regulator want?" to "What would a reasonable person regard as fair?" when considering product design, marketing, sales and after- sales service.

- **Expectations for governance**

  The first outcome of Treating Customer Fairly is an organisational culture in which fair customer treatment is central. Firms can therefore expect the evaluation of the effectiveness of board of directors and senior management charged with overseeing and driving firm culture, the stature and . investment in control functions such as internal audit, risk, and compliance, and the firm's response to

KPMG

incidences of misconduct. Their focus is directed toward decision-making practices and behaviour as a core aspect of good governance, including risk identification, credible challenge, and early intervention. Lessons learned, and risk factors identified during investigations should be further integrated into the ethics / conduct risk program to facilitate root cause analysis across cases and the potential need for follow up and remediation, as well as to reflect the degree to which incidences may be indicative of larger and/ or systemic issues.

> **Fair treatment is no longer only the responsibility of the consumer.** Banks will not get away with the "big boy" arguments or the dated maxim of caveat emptor ('buyer beware'). Fairness and the interests of (and outcomes for) the customer will have to be central in the thinking of financial institutions"
>
> Schalk Engelbrecht. KPMG South Africa, Chief Ethics Officer

Key actions

- Establish and operationalise a conduct risk and ethics management framework that:
  - Defines a measurable conduct risk program, including centralised oversight, governance and controls, and clear escalation protocols and reporting;
  - Aligns and integrates conduct risk with the existing risk and compliance program;
  - Clarifies responsibility for conduct risk management between the 1st and 2nd Lines of Defence;
  - Includes risk assessments supported by metrics, triggers, and thresholds and monitoring and testing;
  - Employs behavior analysis models for employees and consumers, including trends analysis;
  - Reports business-level metrics covering client conflicts of interest, market conduct, training sanctions, and breaches.
- Revisit policies, procedures, and escalation protocols to ensure they are clearly documented and sufficiently robust.
- Invest in technology and/or tools to enhance surveillance, monitoring, and reporting.
- Enhance investigations processes to include complaint management, case documentation, root cause analysis, and remediation and further integrate with the conduct risk program.
- Develop and implement sales practices and incentive compensation risk assessments supported by testing and report results regularly to the board.
- Strengthen recruiting and hiring processes; expand employee exit interviews to include conduct and ethics questions.

Consumer Protection

Drivers

— Heightened public awareness of the value and risks to consumer personal data and related regulatory scrutiny and change

— Introduction of the market conduct regulator with a new and enhanced mandate for the supervision of the conduct of business of financial institutions

— Growing expectations by consumers for transparency and full disclosure on product features and services

— Consumer demand for suitable and personalised products and provision of fair and appropriate services

Challenges

Consumer protection has in recent years taken on renewed focus and attention across all sectors of the financial services industry in South Africa and this elevated focus will certainly continue into 2019, led by the implementation of market conduct regulation under the Twin Peaks regulatory framework. The FSCA's primary mandate, under market conduct regulation, is the protection of financial consumers and ensuring that they are treated fairly by financial service providers that they deal with.

Expectations regarding consumer protection are evolving on all fronts.

For financial institutions consumer protection is far more than just a compliance issue, rather a more strategic approach should be taken. Consumers' growing expectations and resounding social media presence are forcing the agenda, adding to this challenge.

With heightened public awareness of consumers' rights to privacy and the protection of their personal information, consumers are seeking greater control of the processing of their personal information. This is being supported by regulatory changes to consumer protection laws, with the implementation of the POPI Act and the introduction of the GDPR. These laws are putting consumers back in control of their personal information, causing financial institutions to reconsider the purpose for which they are collecting consumers' personal information, and the manner in which they collect, use and retain this personal information.

At the same time, financial institutions must balance the consumers' rights to privacy with the requirement to know their customers. They need to know what their customers want, their needs and preferences, in order to ensure the delivery of appropriate outcomes to these customers. Data and information management is consequently becoming increasingly important to financial institutions in managing the fair treatment of clients.

For a number of years already, there has been a focused challenge in the retail distribution space, with concerns around inappropriate incentivisation; high, opaque and complex fee structures; lack of transparency and disclosure; and design and sale of inappropriate products. The FSB (now the FSCA) has grappled with these challenges through the implementation of the Retail Distribution Review. We are now seeing some of the key proposals of the retail distribution review being given effect to through key regulatory instruments including the FAIS General Code of Conduct, FAIS Fit and Proper Requirements, and the Insurance Acts Regulations and Policyholder Protection Rules. These legislative developments are imposing greater obligations on financial institutions focus on the suitability of the products and programmes.

KPMG

We have started to see a concerted effort by the National Credit Regulator to drive consumer protection in the consumer credit space. We anticipate this will continue into 2019 and beyond. Credit providers would be wise to start getting their houses in order, where they have not already done so.

Key actions

— Develop and implement an effective and clearly articulated conduct risk control framework that requires financial institutions to prioritise the fair treatment of customers and achieving appropriate customer outcomes;
— Conduct consumer protection assessments, particularly related to sales practices and advice, fee structures; suitability of products and services; and remuneration and incentive programmes;
— Invest in tools and capabilities for data and information management, to better analyse employee and consumer behaviours, as well as trends and patterns;
— Evaluate and strengthen data privacy programmes, ensuring that the processing of personal information of consumers and employees aligns with regulatory expectations.

Financial Crime

Drivers

— Digital transformation overall

— Availability of new technologies, including by fintech vendors

— Regulatory expectations for increased integration and improved risk management abilities

— Closer partnership with the business to achieve agility and strategically align initiatives

— Market conditions (cost containment)

— Increased competition from new market entrants and need to innovate

Challenges

The digital transformation, changing how firms operate and deliver value to customers, is driving innovation across financial crimes compliance efforts. Greater agility, efficiency, effectiveness, and resiliency are required today, and firms are focused on automating and integrating their efforts to achieve these goals. Firms also continue to face intense regulatory pressures, increasingly coordinated across multiple regulatory jurisdictions and bodies, to contain attendant risks. In many cases, regulatory authorities expect firms to show greater ability to aggregate data across the enterprise, and understanding of their consolidated financial crimes risks, along with more consistency in their risk management approaches. Independently, firms are struggling to navigate the volume of data and multiplicity of sources and systems (both internal and external).

These challenges are forcing firms to work toward harmonizing financial crimes processes, reducing time per task, eliminating friction, enhancing coordination, and further embedding accountability within the business for financial crimes compliance.

Firms are considering a variety of approaches, including some that are targeted and others that are more extensive, including:

— **Increased standardisation** of methodologies and tools across the enterprise

— **Convergence of controls and teams,** with refined responsibilities across the three lines of defense (for improved risk management)

— **Development of data analytics/ predictive analytics that are aggregated across various types of financial crimes** for a more holistic appreciation of current risks and to better predict future risk areas. Integrating business data and information into the financial crimes picture can provide valuable context as well, enabling greater predictive capabilities when viewed collectively, and optimally in real time

— **Further integration of financial crimes efforts**
AML, sanctions, antibribery and corruption (ABC), fraud, and human trafficking, including integration with the firm's overall compliance risk management efforts. When supported by formalised communication mechanisms, enhanced collaboration enterprise-wide, and aggregation of disparate data, integrated processes improve regulatory reporting abilities and risk monitoring, enabling firms to better predict emerging risks and implement preventive measures.

— **Automation of financial crimes processes**

Repetitive processes, especially due diligence processes related to customer onboarding, transaction monitoring, sanctions and fraud, are ripe for automation, including through use of blockchain technology. By automating aspects

KPMG

of these processes, firms may be able to identify misconduct and regulatory violations earlier in time, achieve greater consistency in output, and improve agility. As with any technology adoption, regulators remain keen to understand the firm's business decision-making process, whether the automation works as intended, any gaps and additional risks created by the technology, and the governance structures in place.

Firms face additional challenges from:

- South African regulatory developments (particularly the FIC Amendment Act) leading to a strategic approach to regulatory compliance
- Organisational needs for cost containment and other resource constraints
- Employees who are not "cultural fits"
- The quick pace of business changes that can present financial crimes risks outside firms'
- Risk profile and tolerance, such as changes to asset classes (organic or through mergers/acquisitions), products and services, transactional activity including use of cryptocurrencies, or to the customer base — notably, the availability of large volumes of customer data and the growth of online transacting can present increased cybercrime risks and fraud risks in credit cards, which require more collaboration and coordination across the enterprise to manage and address.

Key actions

- Evaluate what additional data analytics and emerging technologies can enable your firm to more predictively detect and respond to financial crimes risks, including from business data.
- Discuss the potential to automate certain compliance processes, such as fraud monitoring, in consideration of your firm's enterprise-wide strategy (if any), automation goals, timeline, regulatory risks, and availability of data.
- Determine how to further integrate financial crimes processes or structure for greater agility, cost savings, consistency, and refined risk evaluation.
- Plan for potential regulatory changes on the horizon—ongoing sanctions refinements, expectations for monitoring and reporting human trafficking and for potential shared platforms/arrangements.

Capital and liquidity

Drivers

- Regulatory focus on recalibrating existing regulations to focus on risk, increasing the level of "tailoring" in current rules
- Generally strong capital and liquid assets levels across the industry
- Regulatory focus on financial stability risks associated with counterparty credit
- Proposed guidance has created further 'tailoring' of capital and liquidity rules

Challenges

Throughout 2019 most banking organisations will face a shifting landscape of capital and liquidity-related regulatory requirements brought about by Basel 4 (completed in December 2017 and is due to be implemented from January 2022) and The Basel Committee's recent finalisation of its standards for the capital treatment of market risk.

Basel 4 includes substantial amendments to the capital treatment of credit risk, operational risk and the credit valuation adjustment, the imposition of an output floor, revisions to the definition of the leverage ratio and the application of the leverage ratio to global systemically important banks. Within the South African market, the majority of the banks have already implemented Basel 3 and are sufficiently capitalised with net stable funding ratios (NSFR) and Liquid Coverage Ratios (LCR) in excess of the regulatory requirements. The new Basel 4 requirements will, as a whole, increase the capital requirements.

While banks will be glad that the Market Risk Standards have been finalised, these too will most likely result in capital requirement increases.

During this period of transition, banking organisations may be challenged in the following areas:

- **Credit risk changes**

  The standardised approach has become more granular and risk sensitive. The Committee is removing the option to use advanced IRB for institutions and large corporates, and any IRB approach for equity. Basel 4 will also introduce restrictions (floors) on model parameters.
  These changes will result in higher capital requirements, in particular on higher risk exposures, income producing real estate, and where institutions no longer have the option of the IRB approach.
  There are additional considerations under Credit Risk. The SARB has not, as of yet, confirmed whether they will have their own adjustments.

- **Market risk changes**

  As of January 2019, the Basel Committee has finalised its capital requirements for market risk. The majority of the changes were known to be coming, but banks will still be glad that the uncertainty has now been removed. The major changes, as with credit and operational risk, sit with the modelling approaches. The committee has introduced a simplified standardised approach and recalibrated the current standardised approach (SA) to be more risk sensitive. The largest change, however, is on the Internal Models Approach (IMA) where VaR has been replaced by an expected shortfall (ES) measure. This is to combat the Basel 2.5 tail risk issue which inadvertently incentivised holding positions that featured significant tail risk. The ES method should also better capture market illiquidity in equities and commodities.

Under the new standardised approach, the capital requirements for these will be increasing by 350% and 90% respectively. Interest rate risk and FX risk will increase by 30% and 20% respectively.

It is also clear that the Committee would prefer banks to be on the IMA. Proposed revisions to the Profit and Loss Attribution (PLA) framework (relaxing of test metrics) and amendments to the NMRF treatment (simplified calculation, limited diversification benefits, amendments to quantitative conditions for eligibility for modelling) have made the IMA a much more attractive approach for banks.

— **Credit valuation adjustments (CVA) changes**

New approaches in the form of the new basic (BA-CVA) and standardised approach (SA-CVA) with regards to CVA for derivatives and securities financing transactions have been introduced. As with the Credit Risk, the removal of advanced approaches could result in an increase in capital requirements

— **Operational risk changes**

The largest change on the operational risk side is the removal of the internal model-based approaches. In the South African context, while the SARB has granted approval for the Advanced Measurement Approach (AMA), it has been loath to allow banks to fully realise the capital benefit.

With the new Basel requirements, the AMA approach will no longer be allowed and banks will be forced onto a single Standardised Measurement Approach (SMA). This will raise capital requirements for banks currently on the AMA, but as few SA banks were realising the full AMA benefit, it will not be a large increase. Additionally, the AMA had strict reporting and data requirements. Banks moving from AMA to SMA may be able to save on the costs associated with the data requirements. For banks with large historical operating losses, the new SMA could result in increased capital requirements.

— **Leverage ratio changes**

On the Leverage Ratio side, there are two main changes. Firstly there are revised exposure definition, specifically in terms of derivatives, some off-balance sheet items and holdings of reserves at central banks. Secondly, the Basel Committee is introducing a G-SIB leverage ratio buffer which will be set at half of the bank's capital ratio buffer.

The impact of the definition changes will result in lower capital charges, but for those G-SIB banks, the introduction of the buffer will exceed any benefit, resulting in an overall increase in capital requirements.

CET 1 changes

While the increases in Credit, Market, Operational, CVA and Leverage Capital requirements are expected, there are likely to be decreases in the CET1 requirements. While this will provide some relief for European banks, the impact will be muted on the South African side where bank's total available capital is heavily skewed to the CET1 side, with much smaller Tier 2 reserves than is common in Europe.

Contact us

Pierre Fourie
Partner:
FS Audit Jhb
T: +27 82 490 8077
E: pierrejnr.fourie@kpmg.co.za

Alison Beck
Partner:
Financial Risk Management: Jhb
T: +27 82 492 2709
E: Alison.Beck@kpmg.co.za

Kerry Jenkins
Partner:
Risk Management: National
T+27 83 297 1197
E: kerry.jenkins@kpmg.co.za

Mark Danckwerts
Partner:
FS Audit: Jhb
T: +27 82 710 3261
E: mark.danckwerts@kpmg.co.za

Schalk Engelbrecht
Chief Ethics Officer:
Risk Management: National
T: +27 82 7137656
E: Schalk.Engelbrecht@kpmg.co.za

Nikki Pennel
Associate Director:
Tax - Legal: Jhb
T: +27 82 719 5916
E: nikki.pennel@kpmg.co.za

Malcom Jewell
Partner:
Risk Management: National
T: +27 82 683 5505
E: Malcolm.Jewell@kpmg.co.za

Melanie Miller
Partner:
Technology Advisory: Jhb
T: +2782 717 0195
E: melanie.miller@kpmg.co.za

Roy Waligora
Partner:
Forensic
T: +27 73 622 2319
E: roy.waligora@kpmg.co.za

Michelle Dubois
Senior Manager:
Regulatory Centre of Excellence
T: +27 83 275 2403
E:michelle.dubois@kpmg.co.za

Finn Elliot
Associate Director
Tax-Legal: Jhb
T: +27 79 039 9367
E: finn.elliot@kpmg.co.za

Maria Van der Valk
Partner : Financial Risk Management: Jhb
T: +27 82 712 7878
E:maria.vandervalk@kpmg.co.za

Contributing authors:
Kerry Jenkins, Roy Waligora, Melanie Miller, Maria Van der Valk, Nishen Bikhan, Nikki Pennel, Finn Elliot, Schalk Engelbrecht, Cezanne Krieg, Michelle Dubois, Alisdair Donaldson and Joana Abrahams

kpmg.com/socialmedia

Download on the App Store

kpmg.com/app

KPMG