KPMG

Ten key regulatory challenges of 2020

Financial services risk across business imperatives

kpmg.co.za

Contents

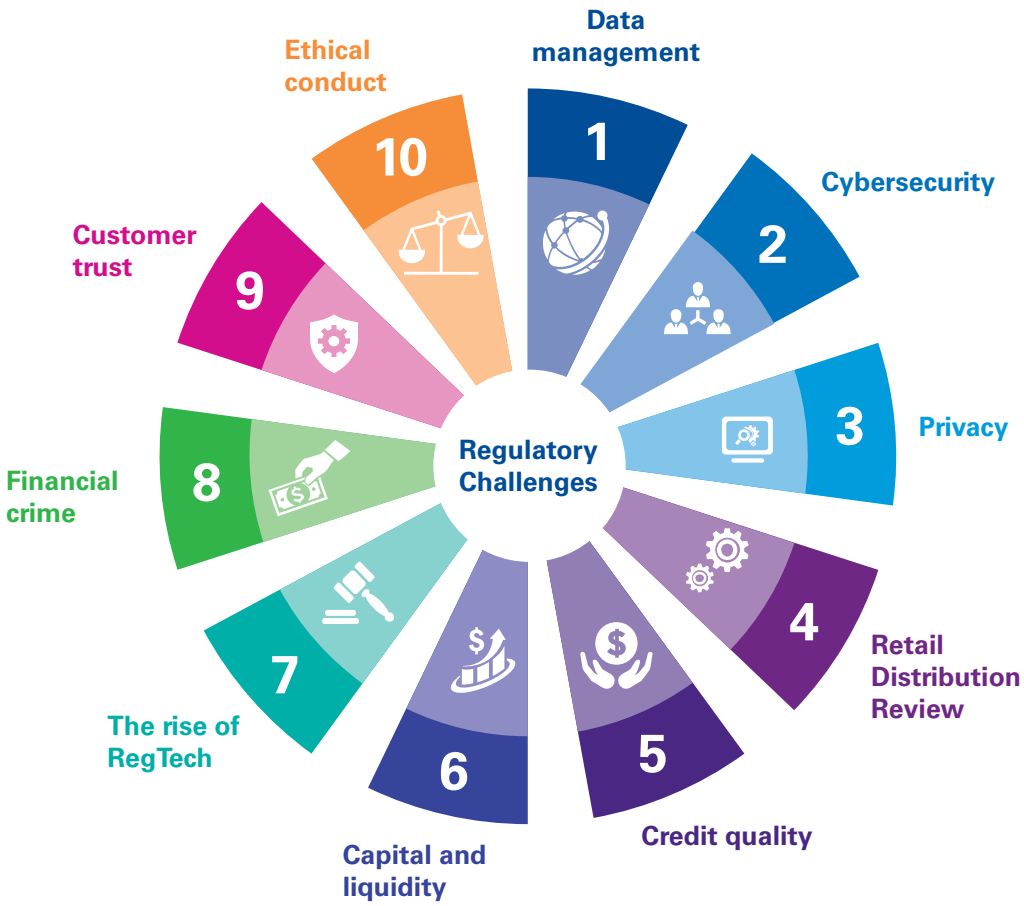
Introduction

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

Regulation continues to drive the strategic agenda. Organisations are required to manage the raft of new rules put forward by global, regional and national policy setting bodies that are changing the structure, supervision and governance of how they operate. Implementation of complex regulatory changes is forcing businesses to change the way they operate while pressure from stakeholders, the market and the competition is already driving change.

Shareholders are demanding that management evidence their ability to meet regulatory demands with limited resources, margins are tight and the pressure to differentiate in a competitive market is intense. In 2020 and beyond, increased regulator scrutiny is expected to continue, particularly in the financial services sector. 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. Regulators will increasingly assess how firms are adapting to market pressures and managing the associated risks, focusing on firms' 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 2020:



1 **Data management:** Expect disruption and embrace business change

2 **Cybersecurity:** Plan for the unexpected impact

3 **Privacy:** Protect your data as the asset that it is

4 **Retail Distribution Review:** Solutions now for streamlined compliance

5 **Credit quality:** Apply the learnings from prior credit cycles

6 **Capital and liquidity:** Easing buffers doesn't mean weakening risk management

7 **The rise of RegTech:** Needing to do more, better, and with less

8 **Financial crime:** Being vigilant to evolving threats

9 **Customer trust:** Trust is critical in attracting and retaining customers.

10 **Ethical conduct:** Do the right thing, even when no one is looking

Data management

Drivers

- Increased importance of trust relationship with customers and regulators
- Recognising and treating data as an asset driving value for the organisation
- Regulatory compliance directly and indirectly calling for better management of data
- Increased focus on overall efficiency and reducing operational costs

Expect disruption and embrace business change

Trust has always been at the heart of the relationship between financial services organisations and their customers. Data and analytics has traditionally played a pivotal role in building and strengthening this trust relationship by allowing organisations to better manage their risks and provide tailored personalised services to their customers through KYC (Know Your Customer) programmes. Today, the sector is pushing the boundaries by using more unconventional data sources and advanced technologies such as Internet of Things (IoT) devices and machine learning to manage risk, inform strategic decision making and drive the customer experience.

The sector has also seen the release of a number of regulations and legislation calling for the effective management of data e.g. BCBS239, SAM, POPIA, GDPR and PPR to name a few. The sensitive nature of data as well as the need to comply with the host of regulations and legislation has created a complex risk landscape that can become difficult to traverse without trusted data and analytics.

It is clear that as the sector becomes more regulated and data-driven, the trustworthiness of their data and analytics will play an exponentially increasing role to underpin the trust relationship with customers and regulators.

Effective and co-ordinated data management serves as the backbone of establishing and maintaining trust in data and analytics. Data management refers to the function of planning, controlling and delivering of data and information assets and aims to maximise the strategic value the organisation derives from its data assets.

Lack of trust in data and analytics

Even though, trust in data and analytics plays a key role in the trust relationship with customers and regulators, it is clear that organisations are reserved in fully trusting and acting on the insights provided by their data and analytics. The recent KPMG International Guardians of Trust study highlighted that only 35% of executives surveyed had a high level of trust in their organisations use of data and analytics. The level of trust varies across the data analytics lifecycle. The highest level of trust being at the beginning of the lifecycle (at the data sourcing stage). However, this trust erodes drastically when it comes to the implementation of analytics models and algorithms to achieve business outcomes.

To address the issue organisations will need to ensure their data management initiatives provide better governance over statistical and algorithm design, maintenance and quality assurance. It should also contribute to greater transparency and understanding of the analytics lifecycle and how it is used to deliver value to the organisation.

Data is an asset with measurable economic value

Organisations acknowledge the importance of data and analytics to improve efficiency, support innovation and growth and comply with data driven regulation. Furthermore, most organisations recognise and refer to their data as one of their most

Wynand Du Plessis
Senior Manager
Emerging Tech
T: +27 82 718 8439
E: wynand.duplessis@kpmg.co.za

KPMG

important assets. However, very few currently formally recognise data as an asset on the organisation's balance sheet, even though it meets all the relevant criteria. This is mainly due to current limitations in quantifying the value of data and a lack of appropriate accounting and asset management practises.

The discipline called "Infonomics" seeks to answer this challenge by providing standardised principles and methods to measure the economic value of data. Formally recognising data as an asset with a measurable economic value will require rigorous management of data value influencers such as data accessibility, data quality, data security, metadata and reusability of data.

Organisations will have to challenge their current data management practices to ensure they are be able to meet this requirement.

Data governance

To ensure the successful implementation and embedding of data management within the organisation, it is critical to establish the relevant data governance support structures that will provide the required top management support, authority, oversight, co-ordination and execution of data management activities. However, many organisations still view data governance activities as a tick-box exercise believing that establishing the role of Chief Data Officer (CDO) and data governance functions, such as the Data Governance Council (DGC) and related steering committees and forums, will inherently result in sound data governance and management. To achieve this, the data governance function requires a clearly

Key actions

— Start with the basics - undertake an initial assessment to see where trusted data and analytics is most critical to your organisation and focus on those areas

— Create purpose: clarify and align data and analytics goals, create clarity around the purpose of data and analytics and demonstrate alignment with the organisation's strategic objectives

— Make the performance and impact of data and analytics impact measurable to build trust in and show Return on Investment (RoI) on data and analytics investments

— Clearly define roles and responsibilities for all relevant stakeholders and provide the necessary education and guidance to allow them to fulfil their responsibilities related to data management and governance

— Encourage increased governance and transparency of the 'black box' by ensuring all business critical and high-risk algorithms have a human partner who is accountable for their performance and impact

— Raise awareness: increase internal engagement, build awareness and understanding of data and analytics across the organisation, including executives, business users, D&A leaders and IT. Also focus on building data and analytics expertise, culture and capability

— Don't let the board off the hook ultimately, executives and boards remain responsible for the actions and inactions of organisations. Educate them in data and analytics risks and controls

defined mandate with roles and responsibilities defined for each of the support structures as well as the representatives serving each of these structures. A sound communication, training and awareness plan is an imperative to educate and equip representatives with the required knowledge and skills to effectively fulfil their data governance and management responsibilities. Further to this, many CDO's are given the C-level title but are not afforded the same level of authority and decision making autonomy as are other C-level executives which can create severe obstacles to achieving strategic data objectives.

If data governance and data management is to be taken seriously and be successful in supporting the organisation in achieving its strategic objectives, organisations will need to profile the role of the CDO as a true C-level executive. Furthermore, data governance support structures, such as the DGC and steering committee, should be recognised and treated as an integral component of corporate governance.

Data strategy

The data strategy is critical to plot the course the organisation will pursue with data management and data initiatives. It defines what data management means to the organisation and assimilates the effective risk management, resourcing and roadmap to assist the organisation in achieving its overall strategic goals. Given the importance of a data strategy it is concerning to note that a KPMG study into trust in data and analytics revealed that only 51% of decision makers responsible for setting strategy for data and analytics, believe their C-suite executives fully support their organisation's data strategy. The main driver behind this is the fact that the data strategy does not provide clear measurements to demonstrate the effectiveness of data and analytics initiatives in achieving business outcomes. If this is not addressed it can create a cycle of mistrust that resonates down into future data and analytics investments and their perceived returns.

> "Trust underpins everything we do as companies, as people and as society. Organisations need to start by creating a solid foundation of trust within their D&A so that when the time comes to 'step on the gas', they can accelerate their initiatives and objectives with confidence."
>
> Christian Rast, Global Head of Data and Analytics

Cybersecurity

Plan for unexpected impact

Financial services has been a key pillar in traditional as well as modern economies. In the last few years, the industry has seen a major disruption from non-traditional players. Consumerisation of technology has led to automation of front office operations which were once considered to be best managed by human operators.

With the evolution of digital technologies, financial service operators increasingly face competition with more agile digital disrupters such as Digital Banks and fin-tech operators. These new entrants are providing similar or better personalised experience to customers at lower costs, by leveraging the power of data analytics, machine learning and cognitive automation. The pace and agility of these new entrants to launch bold new products has forced the traditional players to innovate their systems and processes.

The fact that the new entrants do not have to carry the burden of legacy systems, poses additional challenges to the IT teams in traditional banks. They carry the burden of managing the security implications of newly adopted systems, while simultaneously dealing with the legacy of ageing systems and sunk investment. It also adds complexity to cyber risk management, which is still in its relative infancy.

Involvement of regulators in privacy and security requirements has increased the cost of operations in the short term but it will hopefully result in business being conducted ethically and efficiently, ultimately affording customers' better protection.

Key trends and cyber risk challenges in the financial services industry include:

— **Digital transactions:** South Africa has been ahead or at least on par with other African nations, in the adoption of cashless payments, with almost all merchants, especially in affluent neighbourhoods, accepting credit or debit cards for purchase. User penetration in the Digital Payments segment is expected to be 63.9%, with total transaction value amount to USD 9175 Mn in 2020.[1]

To provide a superior customer experience, financial services organisations are embracing robotics, AI, Blockchain and real-time data analytics. The new faster payment systems and Open Application Programming Interface (APIs), ushers in a new spirit of competition in the banking domain. With the introduction of AI and biometrics used for customer identification and management, financial services organisations have to keep a close eye on fraud and be aware of ever-changing fraud scenarios.

Cyber criminals are already using new and advanced methods to manipulate security weaknesses and traditional security mechanisms may not be sufficient to deal with highly advanced, technology-enabled attacks.

We expect to see more financial service organisations embed cyber security into their digital and business strategy, investing in cyber security as part of the innovation budget and creating a holistic process to become more resilient to evolving cyber

Drivers

— Increased adoption of AI and machine learning in business operations

— Changing regulatory environment with global implications

— Increased awareness and appreciation of boards and senior executive towards cyber security

— Involvement of external participants in managing business processes

— Changing role of technology and security teams in routine businesses

Rupesh Vashist
Associate Director
Tech Assurance
T: +27 66 101 6590
M: rupesh.vashist@kpmg.co.za

KPMG

[1] https://www.statista.com/outlook/296/112/digital-payments/south-africa

threats. Indeed, cyber security will likely become a part of every digital adoption.

— **Involvement of regulators:** With the increase in local and international regulations in business operations, financial services providers in South Africa are striving to keep pace with regulatory requirements. Most of the major banks in South Africa provide app based services and in the process they possess and process large amounts of sensitive customer data. Implementing controls for only rightful use of the data and subsequently protecting this data, remains a challenge for institutions.

  Regulators around the world are becoming increasingly demanding in their expectations of how financial services organisations protect the data collected. They expect the same degree of control a financial services organisation has over its third parties as it has on its own internal operations and processes, to demonstrate controlled usage of data collected.

— **Managing third parties:** Financial service operators including banks and insurance providers, rely on third parties for managing systems and processes. There has also been increased reliance on data analytics vendors to gain meaningful information and intelligence from the vast amount of data collected. In this environment, institutions are pondering how to govern and retain control of these processes which often contain worksteps for third parties to execute, requiring volumes of data, which often contains sensitive information, to be shared outside the organisation.

  Regulators around the word are issuing guidelines and recommendations for managing data exchanged with third parties. In South Africa, POPIA has specific guidelines on processing of customer data by third parties.

— **Cognitive automation and machine learning:** Cognitive automation is taking off across the financial services sector, powered by new-age AI technologies. Almost all clients are deploying robotics in some shape or form in their back office. There has been increased adoption of such technologies in front office processes as well.

  There is a swing towards machine learning to let the bots determine fraud scenarios; currently they're not smart enough and are missing key triggers. It is also not demonstrated for bots to tie different fraud instances together, as fraudsters are purposely targeting below thresholds and trying alternative approaches such as account takeovers. In response, large financial services organisations are starting to deploy machine learning to identify patterns of fraud behaviour and spot signs of fraud.

Key actions

— Embed cyber security in business strategy, rather than running it as a risk and compliance measure

— Create cyber strategy considering key business and technology risks that are relevant to the industry, there is no one-size-fits-all strategy

— Invest in recruiting and retaining a capable workforce of the future that has multi-disciplinary skills and are able to detect anomalies in algorithmic output

— Incidents are inevitable, create an effective crisis management plan, in addition to efforts and investments in preventing the incidents

— Adopt the right tone at the top and cascade the messages correctly

— **Changing role of security leaders:** The traditional Chief Information Security Officer (CISO) role is breaking up. Simply telling the Board how many vulnerabilities were discovered during the previous reporting periods does not really give a full picture of cyber risk. Regulators are viewing security leaders, CISOs and heads of cyber security as owning risk policy all the way through to control and implementation. In the US, the Office of the Comptroller of the Currency (OCC) and the office of the Federal Reserve are telling big financial services organisations that first-line risk should move to a new role of Head of Cyber Risk. Given that they're reporting either to the Risk Committee or to the Head of Operational Risk, regulators want cyber risk to be part of the operational risk framework, with separate reporting. The ultimate goal is to have someone in the risk organisation creating policy and risk appetite statements and lines of business objectives, and having the business approve them.

— We're seeing a challenger to the CISO role and consequently other traditional first-line defence positions are moving to second line, like fraud risk and fraud operations.[2] This is leading to a convergence of fraud and cyber risk. We are starting to see fraud data, anti-money laundering (AML) data, cyber security operations data, and threat-hunting data all fused together in one place as second-line risks.

How we make algorithms secure, when classic programming technology controls are no longer applicable and the logic behind the AI is becoming increasingly complex and inscrutable, remains a critical unanswered question? While organisations are finding it difficult to manage compliance around spreadsheets, it will be even more challenging with robotics operations and straight through processes.

[2] hhttps://na.theiia.org/standards-guidance/Public%20Documents/P%20The%20Three%2 Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

Privacy

Protect your data as the asset that it is

South Africa seems to be inhabiting a regulatory version of Groundhog Day [1] when it comes to the debate on when the Protection of Personal Information Act of 2013 ("POPIA") will come into effect. Facing a 7-year hiatus from the date of the promulgation of POPIA, we still await the President's announcement of the effective date for the substantive provisions of the Act.

It is this semi legislative vacuum, which has perhaps brought about the greatest challenge to local business in terms of determining its approach to data protection.

While it is perhaps not appropriate to compare the progress of POPIA with the long-established data protection regime of Europe, the fact that the European Union is about to celebrate the second anniversary of "new" GDPR [2] is a stark reminder of how embryonic our data protection regime is.

In November 2019, the European Data Protection Board published its Guidelines on Article 25 of the GDPR setting out its recommendations on how business should approach data protection (and privacy) by design and default ("**the Guidelines**"). The Guidelines are useful to guide South African businesses, in the absence of a POPIA effective date, in determining "reasonable measures" to be implemented to secure personal information and ensure that the conditions of POPIA are met, particularly when considering the incorporation of new technology and/or processes to improve operational efficiencies and better serve customers.

We have highlighted a few of the key points of the Guidelines below [3].

What is Data Protection by Design and Default?

Data Protection (which includes privacy) by Design and Default ("**DPbDD**") refers to incorporating data protection early into the design of processing operations (which could include, but is not limited to technology) in order that privacy and date protection principles are embedded from inception. Data protection by default refers to the embedding of the principles of privacy and data protection into processing operations of organisations to ensure that, by default, the rights of data subjects are protected.

Under Article 25 of the GDPR, a controller [4] must ensure that data protection is designed into and is a default setting in all processing (whether electronic or manual) of personal data. Controllers must be able to demonstrate that they have implemented the appropriate measures and safeguards in their processing activities to ensure the ***effective*** compliance with the data protection principles set out in the GDPR. The Guidelines caution that it is not enough to implement generic measures for the purposes of documenting DPbDD compliance, those measures and safeguards must be implemented to achieve the required effect of data protection. Accordingly, controllers may be required to determine appropriate key performance indicators to demonstrate ***effective*** compliance.

Drivers

— 4IR, emerging technology and transformation of workplace environments intended to reduce costs, improve operational efficiencies and better serve customers

— Legislative uncertainty surrounding the likely effective date for the Protection of Personal Information Act of 2013 ("POPIA")

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

KPMG

Have "appropriate safeguards" been specified?

Neither the GDPR nor POPIA defines specific standards for the relevant data protection safeguards to be adopted. However this is to be expected as technology continuously advances and the fact that risk is not equal across all business sectors.

Instead the GDPR and POPIA places the onus on the controller (or "***responsible party***" under POPIA) to assess the internal and external risks to personal information and implement safeguards which are "***appropriate***" to effectively meet the requirements of the GDPR/POPIA and protect the rights of data subjects.

POPIA requires that the responsible party takes into account generally accepted information security practices and procedures which may apply to it or which are required in terms of specific industry or professional rules and regulations.

The Guidelines specifically state that there is no requirement as to the sophistication of a safeguard, as long as it is appropriate to implement the data protection principles of the GDPR ***effectively***.

Key actions

— DPbDD should be considered at the **initial stages of planning** for new technologies and processing operations to reduce wasted and unnecessary costs. A privacy impact assessment should be undertaken to understand the data protection risks of any new technologies and processing operations and the extent to which data protection is embedded by design and default

— Measures and safeguards should be designed to be robust and scalable to handle evolving risks

— Regular data protection impact assessments should be undertaken and safeguards updated to handle new risks or deficiencies in previously implemented safeguards

— Service providers should be selected based on their ability to provide systems which support compliance with the conditions of POPIA (and principles of the GDPR, where applicable). When selecting service providers, planning new technology or processing operations, the cost of DPbDD should be considered in the context of the nature and purpose of processing, as well as the likely internal and external risks to personal information in that organisation's control

[1] Groundhog Day was a 1993 film starring Bill Murray as a TV weatherman who is caught in a perpetual time loop, repeatedly reliving the same day.

[2] GDPR refers to the European Union's General Data Protection Regulation, which came into effect on 25 May 2018, overhauling the 23 year old Data Protection Directive 95/46/EC that was previously in place.

[3] This article is in no way intended to be a comprehensive summary of the Guidelines, the full version of which can be found here: https://edpb.europa.eu/sites/edpb/files/consultation/edpbguidelines_201904_dataprotection_by_design_and_by_default.pdf

[4] A "controller", in terms of the GDPR, is the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Cost of implementation of DPbDD

The GDPR requires the 'cost of ***implementation***' to be considered as a factor when implementing appropriate technical and organisational measures. POPIA broadly requires that a responsible party take "***reasonable measures***".

In our view, it is likely that the reference to "***reasonable measures***" in POPIA (in s19) will be interpreted by our Information Regulator to include a consideration of costs in light of the nature and extent of processing of personal information by an organisation, and the severity of the risks which arise from such processing.

The Guidelines provide that when considering the costs of implementation, consideration should be given to resources in general (including time and human resources), and not only monetary and economic costs. The Guideline warns that "***incapacity to bear the costs is no excuse for non-compliance with the GDPR***", but that cost effective measures should be sought to achieve compliance with the GDPR.

Costs must however be managed to ensure that the controller is able to ***effectively*** implement ***all*** of the principles of the GDPR. This will require an assessment on how the processing impacts all rights of data subjects insofar as their personal information is concerned and implementing measures and safeguards which are effective in mitigating against the threats to those rights and the security of that information.

Timing of implementing DPbDD

DPbDD is required to be implemented "***at the time of determination of the means for processing***" under the GDPR. This requires that when a controller is in the process of determining the means to process personal information, it must also assess the appropriate measures and safeguards to implement the principles of the GDPR. From an economic perspective, this assessment should be undertaken **in the early stages** of planning for new processes and technology, in order to reduce wasted costs and business interruption in having to make changes to infrastructure, technology and processing operations (etc.) after these have been designed and/or implemented.

The Guidelines further require a regular review of the effectiveness of these measures and safeguards, which is mirrored by POPIA.

Data has become an exceedingly valuable asset to business. The fact that there still is no effective date for POPIA should not lull organisations into relegating privacy and data protection to an afterthought, particularly when implementing new technologies and means for processing. Planning for new technologies and processes should include privacy and data protection as a priority on the agenda as early on as possible.

Retail distribution review

Solutions now for streamlined compliance

In November 2014, the Financial Services Board, now the Financial Sector Conduct Authority ("FSCA") published the Retail Distribution Review ("RDR"). This review of the way in which financial products were distributed to the market promised to have a far reaching effect. Initially comprising 55 proposals, the RDR has been implemented in a phased approach, supported by amendments to subordinate legislation and fundamentally changing the regulatory framework.

In December 2019, the FSCA released the most recent RDR status update, giving industry a view of the progress that has been made and next steps to be taken by the regulator. Key topics on the horizon include:

RDR Discussion Document on Adviser Categorisation and Related Matters

The initial proposal (Proposal K) on adviser categorisation proposed different types of advisers, with a focus on the adviser/product supplier relationship and the related responsibilities in each category. This categorisation aimed to increase transparency and better equip consumers to understand the services provided by their adviser. In December 2019 the FSCA published an update of this paper focusing on following key areas:

- Exact terminology used for different adviser categories
- Practical implications of two-tier adviser categorisation – agent of a product supplier and a licensed adviser in their own right (sole proprietor) or a representative of licensed adviser firm which is not a product supplier
- Limitation of product supplier agents' advice to home group products and services
- Utilisation of designation 'Independent' and 'Financial Planner'
- Product supplier responsibility
- Consideration of multi-tied advice model for different product classes

The discussion document released in December 2019 invites stakeholder views on the FSCA's updated thinking on various practical implications of the two-tier adviser categorization and related RDR proposals.

RDR Second Discussion Document on Investment Related Matters

The FSCA published a second discussion document: RDR Investment Related Matters in December 2019, which provides an updated version of the original document published in June 2018. The purpose of the second discussion document is to provide feedback to stakeholders, based on responses received from 2018 Investment Document. This aims to streamline the thought process of the FSCA and key stakeholders, by obtaining their input on four key focus areas as follows –

- General investments landscape
- Information on different activities performed under a discretionary investment mandate
- Categorisation of investment advisers within a RDR framework; and
- Implications for remuneration and charging structures

Feedback received from stakeholders will inform further consultation or the development of draft formal regulatory instruments which will then be subject to the normal consultation processes.

Drivers

- An increasing need for transparent costs charged by financial services providers, enabling customers to make informed decisions regarding the products that they purchase
- A growing need for financial awareness and education
- Mitigating the risk of mis-selling and conflict of interests

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

KPMG

RDR Discussion Document on a Remuneration Dispensation for Savings and Investment Products for the Low Income Market (Proposal TT)

Proposal TT has right from the beginning, recognised that some of the RDR proposals may have unintended consequences in the low income market, necessitating the development of a remuneration model to serve product suppliers and intermediaries working in this market. As part of the consultation process, the FSCA has consulted with industry to better understand this market.

The FSCA has commented in their discussion paper that they have considered whether any change to the current commission regulations for these products is required. "In the interests of ease of implementation and avoiding undue disruption to current business models, we propose retaining the current commission regulation model for qualifying insurance products. Once the full suite of RDR remuneration proposals is closer to finality, we will review whether any change to the Proposal TT remuneration regime may be appropriate."[1]

Position Paper – Final Policy Proposals for Conduct Related Requirements applicable to Third Party Cell Captive Insurance Business

In the above position paper, the FSCA identifies conduct risks inherent in insurance business conducted through cell structures. These risks identified by the FSCA include the following[2]:

- Potential conflicts of interest, including the risk of biased advice to policyholders, the risk of mis-selling, the risk of unfair decision-making related to the payment or repudiation of claims and the risk of inappropriate and conflicted motivation to an intermediary to move a book of business into a cell structure where it may derive additional benefits as a cell owner
- Possibly regulatory arbitrage
- Lack of appropriate governance and oversight by cell captive insurers over the business operated in the cell structures in general and over new product development in particular
- Shortage of skills and resources in some cell captive insurers to administer products and a lack of knowledge and understanding of the intimate workings of the various businesses operating within their cell structures ("rent-a-license" type models); and
- Unnecessarily complex complaints processes and escalation procedures within the cell structures, especially identified where the cell owner is a bank or another large institution, causing unfair barriers to policyholders

Key actions

- Simplify complex complaints and escalation procedures
- Ensure appropriate governance structures and frameworks are in place
- Review and revise remuneration structures

The FSCA has further indicated that these risks will be addressed by an additional conduct standard which will be released and prioritised for comment in 2020.

RDR Position Paper on Equivalence of Reward (Proposal RR)

This position paper provides stakeholders with an update on the FSCA's position on the matter of Equivalence of Reward (EOR). These include a policy to be prepared by insurers covering the remuneration of their tied agents and signed off by the Board. Insurers will further be required to submit, as part of their conduct report to the FSCA, the overall EOR ratio, including an exception report. The calculation of the EOR will be drafted into legislation in 2020 and the normal consultation process will apply.

[1] FSCA Discussion Document on a Remuneration Dispensation for Savings and Investment Products for the Low-Income Market (RDR Proposal TT) December 2019

[2] An extract from the FSCA Discussion Document on a Re Remuneration Dispensation for Savings and Investment Products for the Low-Income Market (RDR Proposal TT) December 2019

Credit quality

Apply the learnings from prior credit cycles

In recent years, supervisory activities and regulatory expectations for model risk management (MRM) have been significantly heightened. In response, regulators have increased scrutiny on banks to maintain effective and sustainable MRM programs. This is a trend that's increasingly gaining traction across the globe.

Generally, Model Risk Management (MRM) is the practice of financial institutions to control and mitigate the risk of financial or reputational damage caused by the use/misuse of models, for example due to errors in model development.

Key components of a bank's Model Risk Management include:

DEFINITIONS	— Establishing a common definition of model risk — Differentiating between a model and a tool to determine their corresponding treatment within the MRM framework
MRM GOVERNANCE	— Defining roles and responsibilities (e.g. model owner vs. developer vs. user) — Approvals, tracking of issues and actions, workflow organization
MODEL INVENTORY	— Key components of the model inventory and the responsibilities for maintaining its accuracy and completeness — Model risk assessment and classification/ risk tiering
MRM POLICIES AND STANDARDS	— Providing guidance on minimum standards required throughout the lifecycle of a model (e.g. model development, validation, treatment of vendor models, etc
MODEL RISK REPORTING	— Key risk indicators to be reported to senior management including model inventory statistics and main validation findings

Drivers

— Regulatory or supervisory initiatives for MRM have been increased over the past few years, resulting in more extensive and rigorous set of requirements and expectations than previously existed. For instance – ECB Targeted Review of Internal Model (TRIM) project, OSFI MRM guidance, BOE 4 MRM principles for stress testing, and PRA guidance on governance of algorithms trading models

Alasdair Donaldson
Senior Manager
Financial Risk Management
T: +27 82 719 1636
E: alasdair.donaldson@kpmg.co.za

KPMG

Challenges

While MRM is in existence in most banks, certain challenges still remain.

— **Model risk appetite and associated limits have not been established by most of the banks.** Those banks that have associated limits utilise both quantitative and qualitative metrics.

— **Capital allocation for model risk is uncommon and few banks** establish a reserve/buffer or provision in some form (e.g. set aside a model risk reserve as a component of regulatory or economic capital). In general, banks are including the capital for model risk under the overall operational risk capital.

Part of the issue is the difficulty in identifying and quantifying model risk. This is due to a number of factors, the most common being the limited supervisory guidance on MRM, the absence of metrics to differentiate model risk for each model in a model inventory, the risk culture within the bank, inadequate in-house knowledge of external models and an inadequate audit trail of historical data.

For smaller banks, the lack of skilled resources, new regulatory requirements and cost considerations have been a driver for the outsourcing of model development and validation activities.

— **Common challenges faced in model risk management include** the labour intensive and time consuming nature of model risk management. This, together with the lack of clarity on roles and responsibilities, the lack of skilled resources and unclear supervisory requirements, has made it difficult for banks to get to grips with model risk management. Further complicating the issue is the difficulty in operationalising MRM principles across various business lines and geographies.

Key actions

— **Mostly banks maintain a firm-wide model inventory.** This will vary depending on the nature of bank, distributed lines of business, model types, geographical footprints etc. The independent MRM function and model owners are mainly responsible for maintaining the completeness of the firm- wide model inventory. From feedback from banks, the vast majority of banks have developed their current firm-wide model inventory in-house

— Banks are improving on their model documentation. Regular attestation processes covering the accuracy and completeness of records in the firm-wide model inventory are taking place

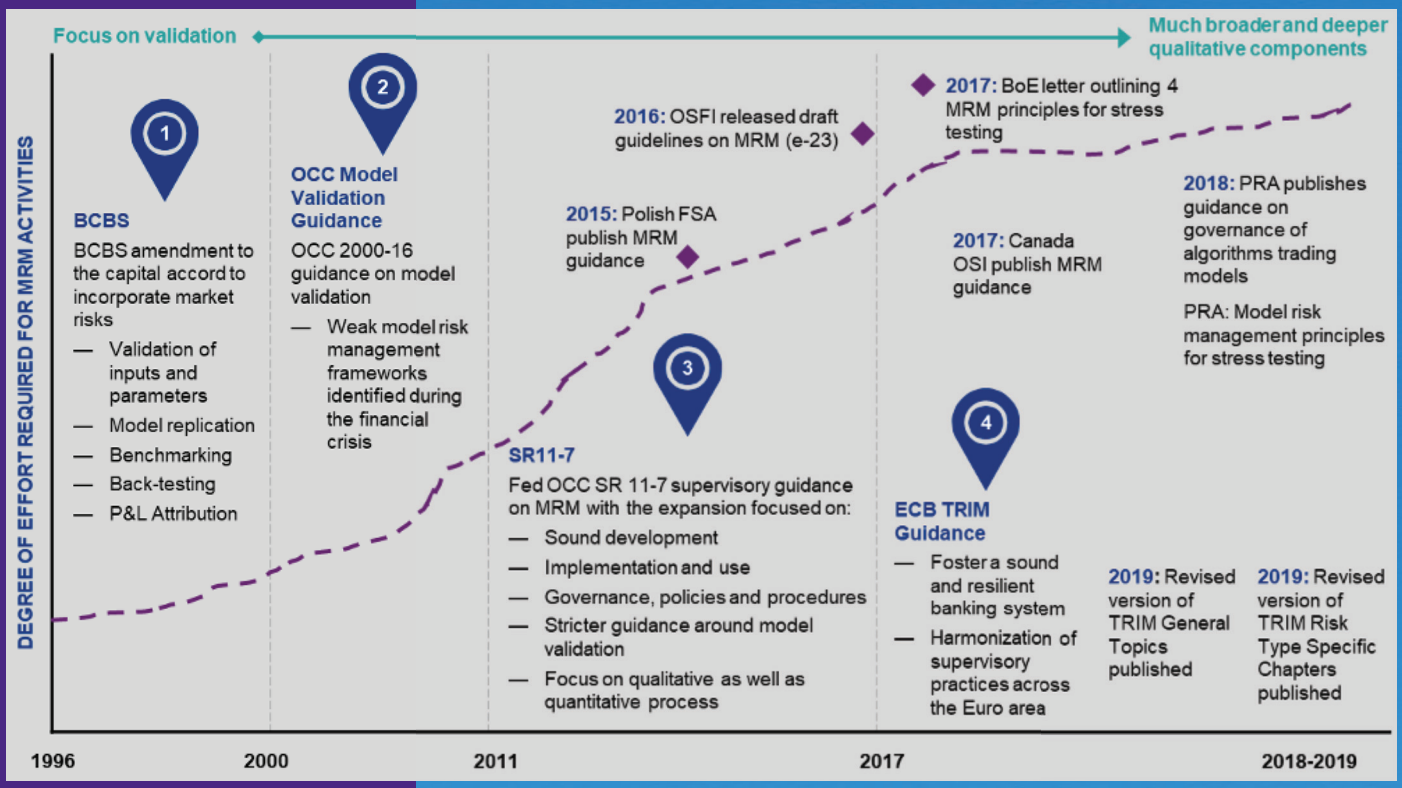
— Model exceptions/waiver processes are being put in place to allow for model usage without the model being validated or formally approved

— Formalisation of the model change process including model retirement/decommissioning is becoming standard practice

— Model governance and culture. Board of directors are usually involved in reviewing or challenging the highest risk tier models along with other critical models. Banks mostly maintain a culture of active model risk management by frequently reviewing their policies, manuals and procedures

— Automation and use of technology. Investing in automated solutions or new technologies to improve model risk management. Through automated solutions or new technologies banks mostly intend to enhance the following areas: workflow approaches for managing model risk (majority of banks), reporting aspects related to model risk management, validation and documentation


5
5


Focus on validation
Much broader and deeper qualitative components
DEGREE OF EFFORT REQUIRED FOR MRM ACTIVITIES
1
BCBS
BCBS amendment to the capital accord to incorporate market risks
— Validation of inputs and parameters
— Model replication
— Benchmarking
— Back-testing
— P&L Attribution
2
OCC Model Validation Guidance
OCC 2000-16 guidance on model validation
— Weak model risk management frameworks identified during the financial crisis
2015: Polish FSA publish MRM guidance
2016: OSFI released draft guidelines on MRM (e-23)
3
SR11-7
Fed OCC SR 11-7 supervisory guidance on MRM with the expansion focused on:
— Sound development
— Implementation and use
— Governance, policies and procedures
— Stricter guidance around model validation
— Focus on qualitative as well as quantitative process
2017: BoE letter outlining 4 MRM principles for stress testing
2017: Canada OSI publish MRM guidance
4
ECB TRIM Guidance
— Foster a sound and resilient banking system
— Harmonization of supervisory practices across the Euro area
2018: PRA publishes guidance on governance of algorithms trading models
PRA: Model risk management principles for stress testing
2019: Revised version of TRIM General Topics published
2019: Revised version of TRIM Risk Type Specific Chapters published
1996
2000
2011
2017
2018-2019

KPMG

Capital and liquidity

Drivers

- Regulation may have become a driving factor behind business decisions
- Banks are exiting once core businesses which do not have favourable effects on regulatory measures
- With so many banks following similar paths, the diversity in products and services between different banks has shrunk. This lack of diversity has possibly increased the risk of the banking sector as a whole

Easing buffers doesn't mean weakening risk management

Nobody likes a backseat driver however this is the very situation banks are facing as increasingly stringent regulatory requirements are beginning to dictate banks internal economic capital allocations.

Economic capital is a bank's own assessment of the amount of capital it should hold to cover a specific risk. This assessment is calculated using the banks own internal models and is meant to match economic realities rather than regulatory and accounting rules.

After the financial crisis it became apparent that banks were too liberal in their estimate of the capital they required and the fallout of that misjudgement has been well documented.

With the intention of avoiding a repeat of this, regulatory bodies implemented various standards which banks need to adhere to. Under Basel III banks must meet various capital and leverage based ratios such as the liquidity coverage ratio and the upcoming net stable funding ratio, while also passing supervisory stress tests such as the FED's Capital Analysis and Review.

An unfortunate result of this is that many banks are exiting once core businesses such as government bond trading and derivatives clearing which does not have a favourable effect on these ratios and regulatory measures. Instead banks are focusing their efforts on business which do.
A 2017[1] presentation by HSBC showed a significant decrease in the number of primary dealers over the proceeding five years, with the most significant being the departure of Credit Suisse from the majority of European government bond primary markets. In the US the results are similar with the number of banks providing clearing services reducing from 84 in the beginning of 2008 to 55 in 2018.

With so many banks following this same path, there have been unintended consequences. The natural diversity one found, with individual banks specialising in areas where they had a competitive advantage is being eroded. This situation has not gone unnoticed by supervisors with Kevin Stiroh the head of supervision at the Federal Reserve Bank of New York, mentioning in a speech[2] that due to the multitude of regulatory requirements banks are facing, they can move towards similar business models and "become systemic as a herd".

The influence that regulators are having is not only confined to banks and their business strategies but has also begun to dominate the topics of discussion among academics and professionals working within the finance and risk industry. A recent article published by Risk.net[3] found that of the 24 papers published on their website over the past year, the number referencing regulatory documents had grown significantly compared with previous years.

Although it is undeniable that banks needed stricter supervision and guidance by regulators and that these rules are having a favourable impact on the ability of banks to weather adverse conditions, there are a number of unwanted results stemming from this. As the saying goes, the road to hell is paved with good intentions and certainly the intention of promoting stability in the international financial system by reducing the damage to the economy banks can potentially cause by taking on excess risk is a good one. But we need to be conscious of the new risks which are presenting themselves as regulation becomes a driving factor behind business decisions.

Chris Shadwell
Senior Manager
Financial Risk Management
T: +27 79 453 9528
E: chris.shadwell@kpmg.co.za

Louis Mukiraine
Senior Manager
Financial Risk Management
T: +27 60 997 4475
E: louis.mukiraine@kpmg.co.za

KPMG

Changes to Banking Regulations?

In December 2017 the Basel Committee on Banking Supervision (Basel Committee or BCBS) published the finalised revised standards to the Basel III framework, which are informally known as Basel IV. The revised standards are to be implemented from 1 January 2022, with some elements thereof (i.e. the Output Floor) to be fully phased in by 1 January 2027. The revised standards focus on the following key components:

Key actions

- Be cognisant of situation where regulatory requirements may unintentionally be driving business decisions
- Start planning for the implementation of the new standardized approach methodology for Market, Credit and Operational risk
- Understand the revised exposure definitions for derivatives and the effect they could have on liquidity ratios

Credit risk

- Revision to Standardised Approach: more granular and enhanced risk sensitivity
- Revision to Internal Ratings Based (IRB) Approaches: Advanced IRB prohibited for institutions and large corporates as well as any IRB for equity
- Input floors: restriction on model input parameters (i.e. introduction of PD, LGD, EAD and CCF floors for corporate and retail exposures)

Market risk

- Trading book vs banking book border: stricter boundary between trading book and banking book
- Revision to Standardised Approach: a simplified standardised approach introduced and the current standardised approach recalibrated to be more risk sensitive
- Revision to Internal Models Approach (IMA): Value-at-risk (VaR) measure replaced with Expected Shortfall (ES)

Credit valuation adjustment (CVA)

- New Basic Approach (BA-CVA): for CVA risks in derivatives and securities financing transactions (SFTs)
- New Standardised Approach (SA-CVA): for CVA risks in derivatives and securities financing transactions (SFTs)
- Enhancement: enhanced risk sensitivity, improved robustness and greater consistency with market risk framework

Operational risk

- Discontinuation of internal model approach: Advanced Measurement Approach (AMA) has been withdrawn
- Revision to Standardised Approach: Introduction of a single standardised approach called the Standardised Measurement Approach (SMA) which uses a combination of business indicators, increasing marginal coefficient and internal loss multiplier

Output floor

- Risk weighted assets (RWA) floor: revision of RWA floor to constrain the extent to which banks can use their internal models to reduce their credit and market risk RWA. Floor calibrated to 72.5% of RWAs under Standardised approaches

Leverage ratio

- Revision to exposure definition: revised exposure definitions for derivatives, some off-balance sheet items and holdings of reserves at central banks
- Global systemically important banks (G-SIB) leverage ratio buffer: leverage ratio buffer set at 50% of G-SIBs' capital ratio buffer

[1] https://www.ecb.europa.eu/paym/groups/pdf/bmcg/171010/2017-10-10_-_BMCG_-_Item%203b_-_Primary_Dealers_-_HSBC pdf?20ac8a7cee0f75bd73ed7d14860ea1ef

[2] https://www.bis.org/review/r181109g.htm

[3] https://www.risk.net/cutting-edge/views/7253271/degree-of-influence-regulatory-policies-drive-quantitative-research

The rise of RegTech

Needing to do more, better, and with less

With technological advances happening at light speed, RegTech is a means of simplifying the process of compliance for firms, automating procedures that were formerly done manually, and streamlining compliance processes to reduce both business risk and the load on human resources.

The volume of regulatory compliance is only going to grow exponentially over time. RegTech offers the potential of innovation and the promise of efficiency which, when embraced could enable organisations to streamline some of the processes involved in reporting, information management as well as risk identification and mitigation.

Drivers

- Growing awareness of reputational and strategic risk
- Challenging market conditions with limited scope to increase headcount means that more must be done with less
- Increased regulator scrutiny and the threat of significant fines for non compliance

A sector under pressure

As FinTech becomes more granular, we see different subsets emerge – one of these subsets is RegTech. RegTech refers to emerging technologies that enable the delivery of regulatory and compliance outcomes, more effectively and efficiently.

RegTech is one of the fastest growing subsets of FinTech and for good reason. The financial services landscape today is challenging. Shareholders are demanding that management evidence their ability to meet regulatory demands with limited resources, margins are tight and the pressure to differentiate in a competitive market is intense. Organisations are under pressure to balance treating customers fairly, do the right thing and ensure favourable outcomes for the man on the street without bowing to social media pressure and risking reputational damage. Financial institutions are turning to RegTech to fill compliance gaps, reduce costs, get ahead of requirements and detect enterprise risk. This means that technology such as advanced analytics, robotic process automation and cognitive computing are not only buzzwords in financial services these days, they are also the future of regulatory compliance in financial services.

Regulators around the world are shifting their focus and engaging actively with RegTech firms. ASIC[1] Commissioner John Price was quoted as saying, 'There is a real need for new regulatory approaches, which is why ASIC strongly supports the development and adoption of RegTech solutions in the financial services sector to provide better outcomes for consumers. RegTech is something we are keenly interested in, both as a consumer of products and a facilitator of engagement more generally to ensure innovation in this area is utilised.' Mark Carney, Bank of England Governor has commented on the increasing regulatory burden, stating that the banking supervision teams at the Bank of England, "now receive the equivalent of twice the entire works of Shakespeare of reading each week."[2]

Earlier this year the Intergovernmental FinTech Working Group (IFWG) published its first FinTech Landscaping Report detailing just how seriously the regulators are viewing the role of FinTech in financial services.

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

KPMG

The aim of the research conducted by the IFWG was to "have a clearer understanding of the FinTech market to enable policymakers and regulators to better manage risk and enable innovation.

It was predicted that RegTech is expected to make up 34% of all regulatory spending in 2020, compared to only 4.8% in 2017[3]. KPMG's recent Market Conduct survey asked participants what measures they were taking to manage their regulatory spend. Almost all participants indicated that employing RegTech was a strategic consideration. Against this background, the scope for continued strong growth in Regtech is clear. Its simply a case of needing to do more, better, and with less.

Key actions

- Develop a comprehensive regulatory landscape
- Refine compliance matrix
- Proactively scan and evaluate regulatory change
- Define problem statements, and identify opportunities to streamline regulatory compliance processes by using technology

> FinTech has the potential to reduce costs and frictions, increase efficiency and competition, narrow information asymmetry, as well as broaden access and to be an enabler for financial inclusion.
>
> Intergovernmental FinTech Working Group (IFWG)

[1] ASIC is the Australian Securities and Investment Commission. ASIC is an independent Australian Government body, set up under and administer the Australian Securities and Investments Commission Act 2001 (ASIC Act). ASIC is Australia's corporate, markets and financial services regulator.

[2] Huw van Steenis, the author of the report "Future of Finance" commissioned by the BoE's outgoing governor, Mark Carney.

[3] KPMG: The Pulse of Fintech, July 2018

Financial crime

Being vigilant to evolving threats

The financial crime landscape is becoming broader and converging across channels. A consolidated approach towards managing these evolving risks is required, incorporating smarter use of technology, alignment with more onerous and complex legislation and adapting to developing trends within the market, economy and broader environment.

Drivers

- Anti-money laundering and Countering Terrorist Finance
- Sanctions
- Anti-Bribery and Corruption
- Tax Evasion
- Market Abuse/insider trading
- Cyber and data security
- Fraud

Organisations need to focus on more than just being compliant with legislation in order to stay ahead of evolving threats and have revealed challenges in the following areas:

— Third party intermediaries:

The risk of transacting with inadequately screened persons and entities, may result in any of the above drivers of financial crime. Increased pressure on organisations to increase business in order to meet targets has escalated the importance of knowing your customer (KYC), related party disclosure and identification of potential conflicts of interest.

— Advancement of technology and the competitive landscape:

Financial institutions are constantly under pressure to innovate in order to improve their services to their clients, as well as stay ahead of their competitors. However, the implementation of new technology and competing with new products in the market can also expose an organisation to financial crime as fraudsters find ways of testing the new systems. Innovation requires an effective governance programme to ensure adequate controls to minimise the risk of non-compliance with legislation and/or financial crime.

— The regulatory landscape

New legislation such as the FIC Amendment Act aims to assist organisations in combatting financial crime by enforcing a risk based approach. However, the impact on business to ensure alignment with such approach and simultaneously maintaining a balance between growth and the associated risks is challenging. Not only penalties for non-compliance, but more importantly, the repercussions on the wider economy can be disastrous.

Dean Friedman
Partner
Forensic
T: +27 82 719 0336
E: dean.friedman@kpmg.co.za

KPMG

Thinking ahead and using financial systems to stop illegal wildlife trade

While the above topics are currently highly prevalent in South Africa and globally, below are some thoughts for further consideration in in order to keep ahead of some potentially other emerging threats:

The financial impact of money laundering and the repercussions on local economies and the fiscus are clear and is hence an important focus area for investigators. However, the proceeds of crime are not always obvious and there is an increasing concern surrounding the predicate offences relating to proceeds of laundered funds. Wildlife trafficking, smuggling and the illicit trade of endangered species for example, the proceeds of which are laundered through the financial system, have become lucrative businesses for criminals.

By expanding on the risk based approach, financial institutions should strive to become attuned to the type of activity resulting in the proceeds of possible crime that flows through their systems and apply tools used to help fight other financial crimes. For example training bank branch tellers and business bankers to better know their customers so that they can spot potentially suspicious transactions that are hidden in perceived businesses that generate large volumes of cash, but in fact relate to the illegal wildlife trade. This is becoming an area of focus for financial crime investigators and Correspondent Banking Academies, who are working with clients to better understand and respond to the illegal wildlife trade. Crimes against Public Interest are however most often cash and trade based driven events, more often than not using trust principles underpinning the flow of transactions, thus making the investigation and prosecution thereof a very complex matter.

Key actions

— Ongoing AML measures

— Fraud prevention, and where necessary advancement in technology. Automaton of outdated processes is continuously required, such as real time fraud alerts, voice/ facial and fingerprint recognition biometrics, and the effective use of artificial intelligence to prevent and detect fraud, while simultaneously ensuring proper governance

— Increase customer awareness in prevention and detection of fraudulent activity. In order to adequately protect customer assets, marketing campaigns designed to heighten customer awareness and highlighting the importance of regulated controls will assist in both strengthening customer rela:onships and combagng fraudulent activity

Customer trust

Drivers

- The importance of a strong corporate culture in building customer confidence and trust through delivery of appropriate customer outcomes
- Regulatory change is transforming the manner in which financial institutions look to meet their regulatory obligations, while the needs and expectations of customers are driving the use of digital technologies
- The customer expectation for a single channel of communication and engagement
- Heightened public awareness of customers' rights to privacy and the protection of their personal information

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

KPMG

Trust is critical in attracting and retaining customers

A sector that has the trust and confidence of the customer will be one that thrives and grows… [Extract from the Regulatory Strategy of the FSCA].

Conduct and Culture

Developing and maintaining a healthy corporate culture is important in managing the fair treatment of customers and ultimately in ensuring customer trust.

A primary objective of financial institutions should be to build and retain customer confidence and trust. This customer confidence and trust will only really be satisfactory when the customer believes they are dealing with financial institutions that value fair, ethical and honest behaviour, that believe in "doing the right thing" for the customer, and where the fair treatment of customers is central to the corporate culture of the financial institution. Strong corporate culture and customer trust go hand in hand.

The 6 fairness outcomes are entrenched in the legislative framework and will form the "blue print" or guiding principles of the new Market Conduct regulations in South Africa. They reflect the manner in which financial institutions' should treat their customers. Primary amongst these is the principle that aims to ensure that *"customers are confident that they are dealing with financial institutions in which the fair treatment of customers is central to their culture."* In fact, the FSCA has indicated its belief that meaningful delivery of the remaining fairness outcomes or Market Conduct principles is unlikely without true commitment to the principle of corporate culture, emphasising the importance of a strong corporate culture in the fair treatment of customers.

Technology Transformation

Financial services regulation is in the midst of a technology transformation and the way that financial institutions respond will have a great impact on both customer experience and customer trust. This is a global phenomenon and South Africa is certainly no exception.

The ever increasing regulatory burden, as new national and global regulation continues to be introduced, is placing financial institutions under significant pressure to manage their regulatory compliance. The regulatory change is transforming the manner in which financial institutions look to meet their regulatory obligations. As the complexity, burden and cost of regulatory compliance increases, financial institutions are looking for new ways of achieving this. With emerging digital technologies, financial institutions are looking to use innovative technologies and digital automation to support their regulatory imperatives.

Customers are also driving the technology transformation. The needs and expectations of customers are changing, demanding digital technology in their channel of communication and means of engagement and interaction with financial institutions, in their products and services; and generally in their customer experience.

As financial institutions embrace this technology transformation, they are expanding their use of

advanced data analytics, artificial intelligence, automation and innovative technologies, triggering further risk and governance adjustments and regulatory attention in areas of consumer protection, the management and security of data; privacy and cyber security.

Customer Interactions

A single channel of communication and engagement with a financial institution is a growing customer expectation and a continuing challenge for many financial institutions. Non-integrated legacy systems across different business areas, customer data housed over multiple databases; interactions across different business lines and even geographies, exacerbate the challenge of creating a seamless customer interaction. As the challenge to meet customer expectations around their interaction with financial institutions continues, so does the struggle to maintain customer trust.

Privacy and Protection

With heightened public awareness of customers' rights to privacy and the protection of their personal information, they 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 similar laws globally (such as the GDPR). These laws are putting customers 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, share and retain this personal information.

At the same time, financial institutions must balance the customers' 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, and the manner in which financial institutions manage customer data talks to the heart customer trust.

Key actions

- Assess the corporate culture within the business and identify indicators to be able to measure corporate culture within the business
- Invest in tools and capabilities for data management, to better analyze employee and consumer behaviours, as well as trends and patterns
- Strive for a 'single view' of the customers that will allow better insight and understanding of the needs and expectations of the customer
- Evaluate and strengthen data privacy programmes, ensuring that the processing of personal information of consumers and employees aligns with regulatory expectations

Can "culture" be measured?

There is no "unit" of culture. Culture does not come in watts or Joules or kilometres per hour. It cannot be counted or numerically represented like revenue.

That does not mean that we cannot generate valid and reliable information about organisational culture. Both qualitative and quantitative data can be collected in order to understand or explain an organisation's culture. This is achieved through, for instance, interviews, focus groups and surveys among stakeholders.

Ethical conduct

Do the right thing, even when no one is looking

The curious relationship between ethics and financial services

Care with financial matters is one of the markers of adulthood – a sign that one is becoming a responsible human being, not only concerned with immediate wants, but also with the future and with the long-term interests of those around you. Savings accounts and insurance policies are consequently associated with (moral) maturity, or being an ethical person.

Ironically, the institutions that provide financial products and services are often not associated with ethics. In cartoons and films bankers and insurers are more often depicted as greedy and remorseless villains who rip off well-meaning customers trying to provide for and protect their loved ones. This unflattering reputation has haunted financial services since biblical times when money-changers were chased from the temple. Fast forward to the Victorian age and one finds that one of Shakespeare's more infamous villains, Shylock, is nothing less than a money-lender. Even in Disney's innocent *Mary Poppins*, it is suggested that bankers' priorities are wrong, and if saving is required, it is to save bankers from themselves.

From Fiction to Reality: A series of unfortunate events

Of course these pop culture depictions are not completely fair. Banks and insurance firms have helped countless people improve their financial wellbeing, buy their first homes, look after loved ones, or get much needed medical help without bankrupting themselves.

Unfortunately, financial services also provide many opportunities for misconduct. This was evident from the recent findings (2018 – 19) of the Australian "Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry". The commission found "conduct by many entities that has taken place over many years causing substantial loss to many customers but yielding substantial profit to the entities concerned"[5].

Examples of unethical conduct included:

— Charging continuing advice fees to customers who had already passed away

— Opening fraudulent accounts in children's names

— Reckless remuneration practices

— Irresponsible loans

These practices are not restricted to a bank or a country. Similar practices have been identified in the United States, the United Kingdom and also South Africa where National Treasury argued in 2014 that financial customers in this country are inadequately protected and vulnerable to abuses that include high fees, unnecessary charges, misselling and reckless lending.

Drivers

— Rewards and incentives

— Conflicts of interest

— Organisational culture

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

KPMG

[5] Commonwealth of Australia. 2019. "Final Report: Royal Commission into Misconduct in Banking, Superannua:on and Financial Services Industry", p.1. Available at hWps://financialservices.royalcommission.gov.au [Accessed: 10 December 2019]

For they know what they incentivise

While these practices do not confirm to the "evil banker" stereotype, they do warn how institutional arrangements within the industry can promote misconduct. The Hayne report, for instance, identified the following causes of misconduct:

— Systems of reward that subordinate purpose (client service) to profit;

— Unchecked conflicts of interest; and

— A lack of attention to organisational culture

These identified causes all boil down to that slippery but crucial phenomenon called "culture", one of the key factors in understanding unethical financial practices, according to South Africa's National Treasury. Reward systems and conflicts of interest are different aspects of an organisational culture. It is slippery because it leads a largely invisible or informal life. But its impact is quite real. Culture is what we unconsciously value, believe and habitually do in an organisation. Culture can also encourage misconduct. It does so in two ways. First, when the culture within an organisation is tolerant of misconduct, employees may abuse the lack of concern to benefit through unethical behaviour. A second, more worrying possibility is when a culture includes the belief that certain unethical behaviours are acceptable or even desirable. This is sometimes referred to as "the normalisation of deviance".

Many factors combine to create a culture, including: the words and actions of leaders; established policies and procedures; performance goals and performance assessment procedures; the language used in the organisation; and, the kinds of behaviours that are praised or judged.

The acknowledgement that incentives, conflicts and culture plays a role in misconduct is not new or surprising. The risk that perverse incentives and conflicts of interest will lead to unethical and costly conduct has been known and discussed for years. What is increasingly exposed, however, is moral hubris in financial services. With regard to both of these risks, the industry has kept believing that "management" or "mitigation" of the risks are possible. As long as we articulate a clear and ethical purpose ("client service", "financial wellness"), and as long as rewards and conflicts are declared, business can continue as usual. The Hayne report suggest differently[6]:

Key actions

— Give ethics, conduct & culture an owner

— Assess the organisational culture

— Identify and assess conduct risks

— Review incentives and reward systems

— Involve leadership

— Make culture and ethics the subject of oversight

> "[Legislation…] speaks of 'managing' conflicts of interest. But experience shows that conflicts between duty and interest can seldom be managed; self-interest will almost always trump duty."

[6] Commonwealth of Australia. 2019. "Final Report: Royal Commission into Misconduct in Banking, Superannua:on and Financial Services Industry", p.2 - 3. Available at hWps://financialservices.royalcommission.gov.au [Accessed: 10 December 2019]

In conditions of conflict, and where both a company and the employees involved in the transactions stand to gain, company missions and values recede into the background. Or, as the report notes, "[p]roviding a service to customers [is] relegated to second place. Sales become all important". This then, is the culture that develops within financial service institutions that rewards sales and profits "… regardless of whether the sale was made, or profit derived, in accordance with law".

Changing conduct (Saving Mr Banks)

So much for the causes of misconduct. How does the industry achieve the opposite? How does one become better, even *good*?

The principle is fairly simple: if you want to run faster, train with people that are faster than you. If you want your conduct to improve, surround yourself with people who conduct themselves well.

For organisations, this means one must create an environment with good examples that encourage exemplary conduct. Put differently, the target is culture. Where conduct is concerned, this has been the refrain – in the report by the Banking Royal Commission, in the requirements of conduct authorities, and in academic analyses of critical failures like Wells Fargo.

This does not make it an "HR problem" or a matter of luck. The culture in an organisation is *not* an accident. Culture and ethics requires as much attention as technical competence.

The basics of culture and ethics are well known:

— Prop up the injunction to act ethically with regular communications from leadership;

— Ensure that sufficient resources are made available for ethics & culture programmes;

— Measure and track your culture;

— Train employees on the values and standards of the organisation, with practical scenarios to habituate good conduct; and

— Ensure that ethics performance is monitored and track, and are the subject of oversight.

In addition to assessing culture, in financial services it is imperative to do conduct risk assessments and to review incentives and reward systems to ensure that reckless behaviour is not encouraged, and the right conduct (conduct that is fair and in the best interest of the customer) is recognised.

These organisational processes are important, but they should not substitute for the common sense principles of financial services. First, "Thou shalt love thy customer with all thy products and services". This is the first and great principle. And the second, which is equal to the first, "Thou shalt not sell what they would not buy thyself, or sell unto thy mother". On these two principles hang all the laws and the regulations.

Contact us

Pierre Fourie
Head of Financial Services
T: +27 82 490 8077
E: pierrejnr.fourie@kpmg.co.za

Joelene Pierce
Head of Financial Services Markets
T: +27 83 291 4217
E: joelene.pierce@kpmg.co.za

Mritunjay Kapur
Head of Advisory
T: +27 71 402 8445
E: mritunjay.kapur@kpmg.co.za

Joubert Botha
Head of Tax
T: +27 83 456 7734
E: Joubert.botha@kpmg.co.za

Michelle Dubois
Senior Editor
T: +27 83 275 2403
E: michelle.dubois@kpmg.co za

We value your feedback and would be delighted to hear your thoughts on this piece of thought leadership. Please reach out to discuss any of these topics in more detail.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia