# Ten key regulatory challenges of 2021

## The future of regulatory: Altering our view

kpmg.co.za

# Contents

# Introduction

## The future of regulatory: Altering our view

The disruptions that faced all industries in 2020 will forever reshape the financial services industry.

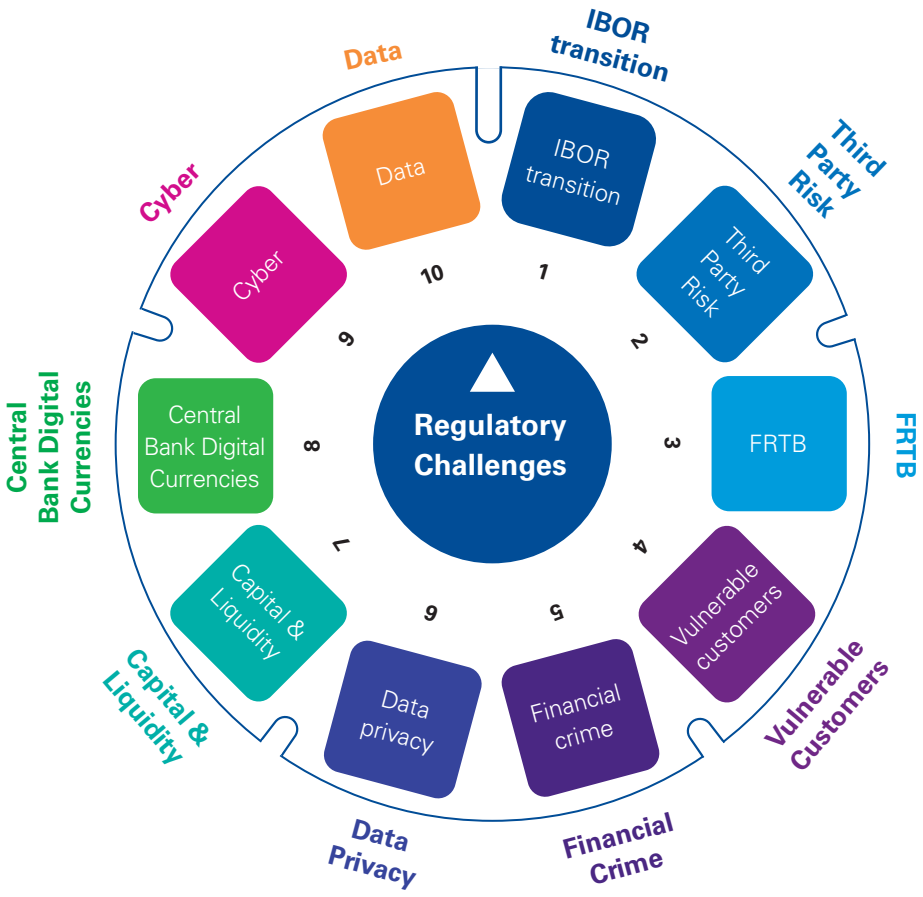
Notable among these are the accelerated use of online and digital technologies, the long term adoption of remote working practices and the demand for adjusted business and risk strategies as the world became a very different place. Together they have impacted all aspects of a financial services company's physical and strategic operations, technology systems and data security, products and services, customer interactions, and third party relationships. With such change comes regulatory challenges and concerns which in 2021 will begin to set forth the future of regulatory: altering our view.

Therefore we present our ten key regulatory challenges for 2021 and help answer the question: What are the steps I can take now to prepare.

**Michelle Dubois**
Senior Manager
Regulatory Centre of Excellence

With acknowledgement to Amy S. Matsuo. National Leader, Regulatory Insights, KPMG US

## KPMG highlights the key drivers and actions for firms in the following Key Ten Regulatory Challenges for 2021:




1. **IBOR Transition:** Replacing the world's most powerful number
2. **Third-Party Risk Management:** Addressing the serious challenge of third-party risk
3. **Fundamental Review of the Trading Book ("FRTB"):** Setting the bar higher
4. **Vulnerable customers:** Ensuring that no man is indeed left behind
5. **Financial crime:** Chasing shadows of illicit events
6. **Data privacy:** Protecting your data as the asset that it is
7. **Capital & Liquidity:** Balancing inherent tensions to weather the storm
8. **Central Bank Digital Currencies:** The evolution rather than revolution of fiat currencies
9. **Cyber:** Protecting the lifeblood of the organisation
10. **Data: Cloud computing and data sovereignty:** The infinite value of data in the sky

KPMG

## Drivers

- Concerns about the core nature of IBORs have been swirling for years
- IBORs are dependent on rate submission by a select group of banks, which are quote-based and can be subject to manipulation. The aim is to move toward transactional-based quotes, which provide more transparency
- Banks no longer fund themselves on the interbank market as before, hence the rate was not as representative as before of the true state on inter-banking borrowing
- The risk that many IBORs could be found to no longer represent the underlying market it is meant to measure, due particularly to a lack of underlying primary and secondary market activity
- IBORs rates are not risk-free, as they include a credit risk premium that reflects the perceived credit risk of the panel of banks that contribute to IBOR, and thus render the benchmark not perfectly suitable for discounting derivatives transactions

**Auguste Claude-Nguetsop**
Partner & Head of Market Risk – IBOR National Lead

# IBOR Transition

## Replacing the world's most powerful number

The discontinuation and replacement of the Interbank Offer Rates (IBOR) by Alternative Reference Rates (ARR) represents one of the most ambitious transformations in financial markets in recent times. Its impact will be far reaching, affecting sell-side and buy side professionals, corporates, and in general any market participants with interest rate benchmark exposure.

Although the official cessation date for IBORs publication is set to December 2021, many jurisdictions such as South Africa are leveraging this regulatory reform to significantly change their internal interest rate benchmark, and are thus planning a separate cessation date for their own benchmark rate.

In South Africa, Jibar is the key benchmark used as the reference interest rate for financial instruments and derivatives; with the three-month Jibar rate being the most widely used and accepted reference for South African Rand-denominated financial contracts. It is estimated that the total value of outstanding derivative and non-derivative contracts that reset against the three-month Jibar rate exceed R40 trillion as-of 2018.

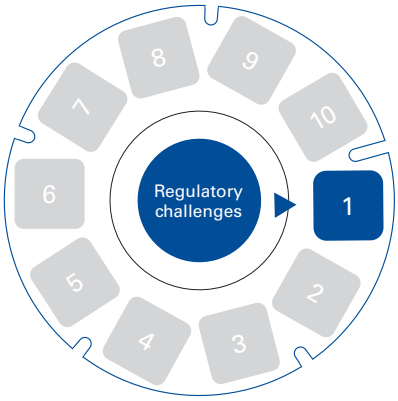
## Transitioning from IBOR to ARR

IBORs currently underpin a huge range of financial products and valuations, from loans and mortgages through securitisations and to derivatives across multiple jurisdictions. They are used in determining all sorts of tax, pension, insurance and leasing agreements and are embedded in a wide range of finance processes such as remuneration plans and budgeting tools.

Despite its popularity, concerns about the core nature of IBORs have been swirling for years, driven primarily by some of those key following factors:

- IBORs are dependent on rate submission by a select group of banks, which are quote-based and can be subject to manipulation (as seen in the 2012 Libor scandal in the UK). The aim is to move toward transactional-based quotes, which provide more transparency.
- Banks no longer fund themselves on the interbank market as before, hence the rate was not as representative as before of the true state on inter-banking borrowing
- The risk that many IBORs could be found to no longer represent the underlying market they are meant to measure, due particularly to a lack of underlying primary and secondary market activity
- IBORs rates are not risk-free, as they include a credit risk premium that reflects the perceived credit risk of the panel of banks that contribute to IBOR, and thus render the benchmark not perfectly suitable for discounting derivatives transactions.

Although the discontinuation date of IBORs is scheduled for the end of 2021, the timeline of the Jibar replacement is still to fully finalised




and communicated. The SARB has however already recommended in Q4 2020 that South Africa transitions to a near-risk free rate as a key overnight reference rate. This means that jibar will, in future, not be used as a key reference rate for financial contracts in South Africa.

To avoid a multi-step transition, the SARB has recommended, as an initial step, that the current jibar framework, including its governance, be strengthened in order to secure the transition period, while the MPG and its work streams continue their work on operationalising an alternative reference rate.

Transition to the alternative reference rate will only take place when the rate is fully functional, which could take up to four or five years. Any measures taken to strengthen the jibar framework during the interim phase would need to ensure that the rate is credible and resilient, until full transition takes place.

## Challenges of IBOR transition

The IBOR transition complexity is driven by the difference in nature between IBORs and ARRs, as well as the significant impact of the transition on market participants infrastructures, legal, operational and systemic risks.

IBORs are forward-looking rates, meaning that a borrower knows the interest rate on a loan at the beginning of the interest period. In contrast, ARRs are overnight indices, implying they are backward-looking and, therefore, require significant efforts to define a term rate structure and a yield curve. ARRs are also designed to be risk-free (i.e. free of any credit risk premium).

In consequence, the ARRs are, in general, expected to be lower than the current IBORs. Further, the ARR will not only be based on the interbank market but will also involve payments made by banks to non-banks. This will increase the number of underlying transactions used to determine the interest rate.

Market participants and professionals should anticipate a period of higher market volatility and liquidity issues following the introduction of newly established ARRs. That could lead to larger than anticipated valuation differences, tax estimations discrepancies and hedge effectiveness breaks.

## Transition Steps

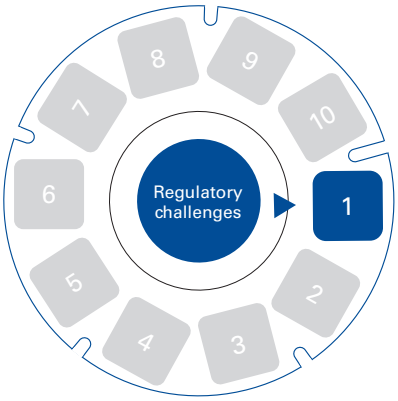
Based on the conclusion of the MPG established by the SARB to assist with recommendations for the replacement of the Jibar and the definition of ARRs , the critical transition first step will be the establishment of the standard overnight reference rate for the ZAR overnight index swap ("OIS") market, using the rate for swap discounting and remunerating collateral. Unlike in the United Kingdom, where this was a straightforward process as the successor rate, SONIA, was already the established reference rate for sterling OIS, significant work will need to be done in the South African market, given that there is currently no liquid market for OIS.

Following the establishment of a liquid market for OIS, the following pillars will be developed as part of the transition journey:

- Derivatives market adoption;
- Adoption in the cash/other markets; and
- the transition of legacy contracts and position.

## In Summary

Although the Covid-19 pandemic has diverted some attention from the drive to meet IBOR transition deadlines, there have not been any plans in any of the leading IBORs markets to delay the transition planned for December 2021. The recommendation made by the SARB to transition to a near risk-free rate through a staged and incremental approach, with a reformed Jibar step in the interim have been co-defined with market participants, thus a guarantee of solid buy-in.




> Although the discontinuation date of IBORs is scheduled for the end of 2021, the timeline of the Jibar replacement is still to fully finalised and communicated. The SARB has however already recommended in Q4 2020 that South Africa transitions to a near-risk free rate as a key overnight reference rate. This means that JIBAR will, in future, not be used as a key reference rate for financial contracts in South Africa

Auguste Claude-Nguetsop,
Partner & Head of Market Risk – IBOR National Lead

## Key actions

— Sell Side: Banks will have to manage conduct, basis, legal, operational and systemic risk. Tax and accounting impacts will also have to be managed. Finally, the key transition challenges on contract remediation, internal and external communication and liquidity for term structures rate will also have to be addressed.

— Buy Side: Corporates, insurers and asset managers will face similar risks and challenges to those highlighted for the sell side. They will also have to deal particularly with cash-flow management and valuation reconciliation issues, as well as financial reporting. Insurers will have to handle risk-free yield curves for solvency reporting purposes as well term structures rates for long dated derivatives transactions.

KPMG

## Drivers

— Ever increasing regulatory expectations for establishing controls over third parties

— In certain instances, the pandemic impacted ongoing monitoring and performance management processes over third parties

**Thomas Gouws**
Partner
Risk Consulting

# Third-Party Risk Management

## Addressing the serious challenge of third-party risk

In today's complex and volatile global markets, third-party relationships are a critical source of competition and growth for financial services organisations. Financial organisations are increasingly reliant on third-party suppliers to deliver business-critical products and innovative services in the fast-paced and ever-evolving digital age.

Third-party risk management ("TPRM") needs to be approached in a more-consistent manner that ideally relies on a centralised and refined service model across the entire organisation. Failures by third parties can rapidly tarnish business reputations, unleash significant downstream operational and cost implications, and generate significant penalties for regulatory non-compliance or misconduct.

## Consider today's volatile environment a catalyst for improvement

Financial service organisations should view today's risk-laden environment as a tipping point toward heightened TPRM awareness, strategy and execution that ensures sustained and consistent third-party assessment, onboarding, oversight and monitoring. A properly functioning TPRM program provides critical insights that include:

— Selection and evaluation of third-party service providers;

— How the third party will access, store and/or transmit the organisation's data;

— Whether third parties maintain a control environment that meets the organisation's needs; and

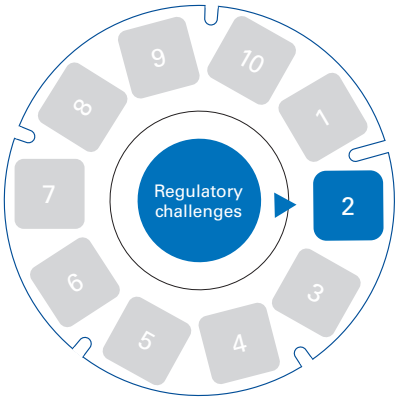
— Which specific requirements need to be negotiated into third-party contracts.

No 'one-size-fits-all' TPRM program exists. Each requires an informed and precisely defined strategy that is supported by a clearly articulated risk appetite.

Holistic risk identification and assessment during onboarding, and throughout the lifecycle of the contract, is crucial to maintaining a line of sight into the risk profile of the entire third-party portfolio. Financial services organisations need to take a risk-based approach to assessing and monitoring third-party products and services that present the highest risk to the organisation. This is particularly true amid today's disruptive COVID-19 environment and on that front KPMG has defined four phases for organisations to consider in response to the pandemic: Reaction, Resilience, Recovery, and the New Reality:

— **Reaction and Resilience:** Implementing emergency moves to remote working models and rapid reconfiguration of third-party service delivery models; and

— **Recovery and the New Reality:** Preparing for subsequent virus breakouts, new government regulations and supplier uncertainty.




Yet many organisations within the financial sector and beyond, still lack the critical technology and skills that underpin effective TPRM programs.

There is no time to lose on the journey to TPRM maturity. Successful TPRM transformation demands strategies that overcome the roadblocks that have plagued systems throughout their initial build and subsequent iterations. These include:

— Inadequate executive support and tone at the top;

— Resistance to organisational realignment;

— Large resource needs to operate the program;

— Insufficient accountability from third-party organisations;

— Lack of investment in technology enablement; and

— Resistance from third parties to co-operate with the TPRM process.

Many financial services organisations still have a long way to go before they reach maturity. True transformation is driven by a constant cycle of program uplifts, process optimisation and innovation. Firms grappling with uncertainty and disruption can no longer ignore these key steps to TPRM maturity:

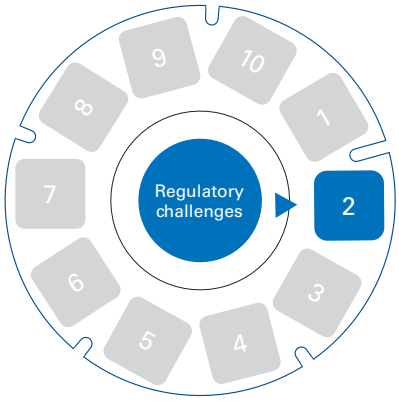
— **Agree on the vision:** A key consideration for an enterprise wide TPRM program is designating program ownership and determining where TPRM sits within the organisation.

— **Build the model:** TPRM programs are complex, meaning development is not a one-time exercise but a work in progress requiring organisations to 'strike the right balance.' Key to efficiency is a centralised and sustainable service-delivery model that facilitates risk assessment on behalf of, and with input from, the business. Financial services organisations may opt to use distributed or centralised models.

— **Optimise the process:** Financial organisations can optimise the risk-stratification process in two ways: **risk segmentation** — establishing a disciplined risk-scoring methodology across third-party services — and **enhancement** of the service-delivery model to reduce costs and increase accountability. Organisations should segment third-parties into three categories: those presenting nominal risk to the organisation and that do not need to be risk assessed; those that are appropriate for the standard TPRM process; and those that present a homogenous risk profile and are more efficiently managed centrally, via a specialty program.

— **Evolve and innovate:** Financial services TPRM programs typically revolve around the gathering and assessment of third-party data. Organisations are focusing their limited budgets on new tools. We see leading TPRM teams using automation, data analytics and natural language processing, as well as incorporating scoring services for affordable and scalable monitoring across select risk areas, performance management, and contract compliance. TPRM programs are exploring how they can use machine learning to evaluate internal data around risk events and identify risk events that may be caused by a third-party. They are automating the monitoring of third-party compliance with SLA terms, identifying opportunities to recoup fees for missed commitments, and taking a more-proactive approach to reputational risks.

Whilst we see more organisations wisely taking a proactive approach to TPRM, it remains a work in progress for many. Financial organisations have no time to lose in addressing the serious challenge of third-party risk and the pressing need for a more-consistent approach that ensures operational resilience.




## Key actions

— A single TPRM program leader with a reporting structure to senior management and the Board;

— An enterprise-wide outsourcing and third-party strategy and a defined risk appetite;

— Clear responsibilities and accountabilities across the TPRM program and lifecycle;

— An inventory of third-party services to which the program applies, with clearly defined services;

— Consistency of execution across the organisation's business units to drive quality data for analysis and integration with the second and third lines of defense;

— A risk-based approach to assessing third-party services, tied to the program's risk appetite;

— Risk assessment and due diligence prior to contract execution and decision-making;

— TPRM technology architecture that supports efficient workflow, task automation and reporting across the entire business;

— A documented and well-understood audit trail;

— A service delivery model that's aligned to the organisation's operating style;

— Integration of TPRM activities and technology organisation-wide into processes, such as procurement, legal and finance, and into existing risk- oversight functions and activities;

— Collection of real-time data around the TPRM program's ability to manage third-party assessment, onboarding and monitoring;

— A comprehensive data model for collection of third-party information, including service details, risk scoring, contract information and performance monitoring;

— Internal data feeds that monitor and record specific events and incidents attributable to third-parties, and external data feeds that monitor for real-time information on the third-parties, such as adverse media, changes in business ownership, corporate actions, cyber vulnerability scores, financial viability ratings;

— A process to update third-party risk profiles when there are changes to the risk score and real-time tracking of performance against service level agreements (SLAs) and real-time tracking of risks against key risk indicators (KRIs); and

— Data-driven decision making, where risk assessments and performance monitoring influence contracts and decisions

KPMG

## Drivers

— The Basel Committee on Banking Supervision has made it clear that a "more coherent and consistent set of rules" is required to "reduce variability in market risk capital levels across banks"

**Auguste Claude-Nguetsop**
Partner & Head of Market Risk – IBOR National Lead

# Fundamental Review of the Trading Book ("FRTB")

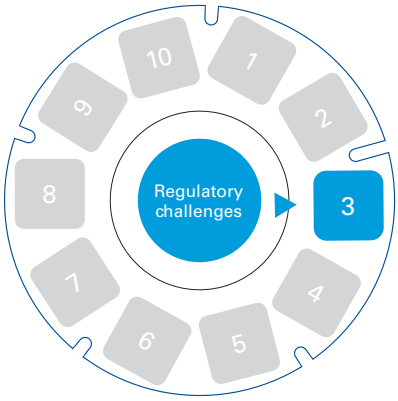
## Setting the bar higher

Despite the Basel Committee's one-year reprieve on the deadline for FRTB implementation, delaying the initial hard deadline of December 2022 by one-year, South African's banks still have much to contend with before January 2023 and the mandatory twelve months back-testing. In addition to complex decisions over modelling approaches, infrastructure, data management and reporting, the banks also must integrate FRTB alongside other regulatory requirements such as SA-CCR and the IBORs transition, which mean a very challenging and narrow path to a successful implementation. Furthermore, the Covid-19 pandemic has added a layer of operational complexity to a host of other challenges to be considered for the FRTB journey.

Under the Basel Committee on Banking Supervision's FRTB, banks have a choice of methods for calculating market risk capital: a sensitivities-based approach (SBA) set by the regulator; a simplified standardised approach (SA); or – if trading desks pass certain tests – an internal model approach (IMA).

The largest SA banks are treading a fine line between seeking a sensitivities-based approach to calculating market risk capital for their trading books – and assessing the use of internal models if the business case provides evidence of potential cost savings. Smaller banks are considering the use of the simplified standardised approach, as it comes with less complexity in its implementation and can provide an optimal cost-benefit ratio in some specific cases. It remains however to be seen if the SARB will allow it given the risk of regulatory capital arbitrage that is posed by the SA approach when selected by a D-SIB.

For the leading banks, the obvious fallback if internal modelling does not reliably yield capital benefits that justify the heavy systems costs, is to adopt the standardised SBA. Most appear already to discard the basic simplified SA approach, as they are willing to make significant investment in new systems to collect risk sensitivities data and upgrade their risk engines capabilities. The simplified SA doesn't require this complex technical infrastructure to run, and will likely be the choice in the African subsidiaries and for smaller local banks.




## Transition to a less volatile risk capital framework

The market turmoil brought about by the Coronavirus outbreak has exposed a double-counting defect in the current market risk framework (Basel 2.5).

To calculate minimum market risk capital requirements, banks add together two versions of VAR. The first is regular VAR, which estimates the losses a bank's portfolio would suffer if it was subject to the worst trading day in the past year. The second is an estimate of losses for the same portfolio if it was subject to the worst trading days in the bank's history, known as stressed VAR.

But as current conditions are a crisis scenario, the requirements are partly duplicated, hence, South African banks have experienced multiple instances in 2020 where their VAR was higher than their Stressed VaR, a clear evidence of the double-counting defect under Basel 2.5.

FRTB promise to address the problem by replacing the overlapping requirements (VaR and Stressed-VAR) with a single measure of risk. However, the new rules could still lead to higher capital than expected from back-testing exceptions.

Overall, as the final implementation date for FRTB has now been delayed to 2023 along with the rest of Basel III as a consequence of Covid-19, gauging the impact remains a way off – and, even then, its true final cost will not become clear until it is thoroughly tested in the next market crisis. It would have been a perfect test of the reliability and suitability of the new rules if they had been implemented prior to the pandemic. The next crisis will be the ultimate real life back-testing of the model and the FRTB framework.

### Key actions

— Banks need to re-look at their data collection, their data transformation and warehousing, their data quality management processes and, in general, upgrade their data management to ensure they can support FRTB demanding requirements on items such as look-through obligations for index and fund constituents

— Banks need to ensure investments are secured and maintained to overhaul their existing risk infrastructures which requires specialised expertise to support the enhanced risk methodologies that FRTB introduces

— FRTB requires that options and embedded derivatives which are issued and held in the Banking book must be transferred and held in the Trading book. That is a sizeable task which needs to be given a high priority as banks need to identify every asset held on the Banking book which contains an embedded derivative. The effort will be comparable to identifying LIBOR related assets in a bank's portfolio

KPMG

## Drivers

- The number of customers identifying as vulnerable is increasing due to tough economic times and the impact of the COVID 19 pandemic
- There is increased regulator scrutiny combined with public pressure on financial services firms to do the right thing, even when no one is watching
- Looking after vulnerable customers is not just a compliance exercise, it's a business imperative

**Michelle Dubois**
Senior Manager
Regulatory Centre of Excellence


# Vulnerable Customers

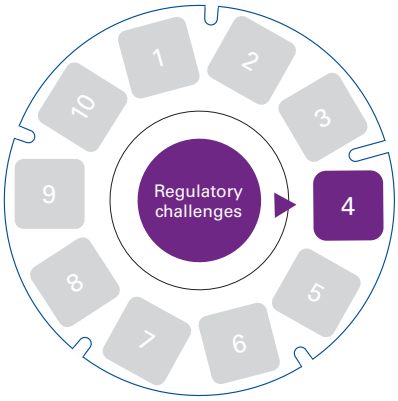
## Ensuring that no man is left behind

The concept of the **vulnerable customer** is receiving increasing focus in South Africa in recent times, particularly as we struggle through difficult economic times and fight the COVID 19 pandemic. The Ombudsman for Banking Services in South Africa has stated that "financial service providers are expected to provide consumers with appropriate products and services and a level of care that has due regard to the capabilities of the consumers in question. The level of care that would be deemed appropriate for vulnerable consumers may be different from that which would suffice for other consumers. It is crucial that financial firms acknowledge this and implement processes and procedures to cater for the needs of vulnerable consumers, as these customers may face a significant risk of harm".

The term vulnerable customer was first defined by the UK Financial Conduct Authority ("FCA") in 2015, as *"someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care."* This definition has two elements to it that we should examine further to ensure a complete understanding of the concept of the vulnerable customer - the first being the customers personal circumstances that may result in them being prone to a greater degree of harm than the average customer; and the second element being the onus that is placed on the financial institution to treat the vulnerable customer fairly and with due consideration of their circumstances.

### Identifying the vulnerable customer

This brings me to question how we identify vulnerable customers and their needs. Defining vulnerable customers is a fluid concept, particularly at a time where this category of customer has expanded dramatically as a result of not only the COVID pandemic, but also as a result of globally constrained economic circumstances. An example which is particularly relevant, at this time when many financial institutions are offering pandemic relief is premium holidays. By their very definition, the customers making use of these offers are vulnerable. Do these customers fully understand the long term financial implications of taking a premium holiday and the implication on the total cost of credit? Is this a short term solution that might come back to bite them later on? More importantly is this a solution which treats the vulnerable customer fairly and gives them a sustainable financial solution?




In the same way, we must consider the impact of rising unemployment; short term income reduction in numerous sectors as various stages of lockdown are implemented; and the impact of illness and economic uncertainty. It might be a short-term concern or it may be ongoing, so our existing parameters as financial institutions need to take cognisance of this.

## The onus on financial services firms

Taking the guidance from the FCA one step further, the FCA explains further in their definition that, "vulnerable consumers may be more likely to experience harm. In many cases, this risk of harm may not develop into actual harm. But if it does, the impact on vulnerable consumers is likely to be greater than for other consumers."

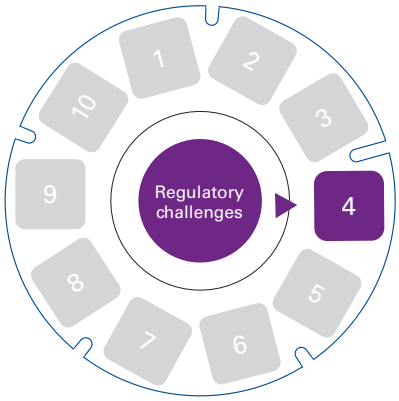
That's a big "if" and raises the question to what lengths should a financial services firm go to, to ensure that vulnerable customers are identified, protected and ultimately treated fairly? What increased responsibility or onus lies with the financial institution to consider or ensure appropriate outcomes for the vulnerable customer? The FCA, which is closely followed by other jurisdictions, and in particular our own, is increasingly indicating that they are looking for financial institutions to show that their products and services remain relevant for their customers, even in changing circumstances.

The second draft of the Conduct of Financial Institutions Bill ("the Bill") released in 2020 makes it clear that when providing financial products and financial services a financial institution must ensure that the products and services are— (a) appropriate for targeted or impacted financial customers; (b) provided in a manner that is as objective as possible; and (c) provided in a manner that supports the delivery of appropriate financial products and financial instruments to those financial customers.

The Bill goes further to say that a financial institution must ensure that its financial customers are provided with financial products and financial services, as the case may be, that perform as that institution has led its financial customers to expect, through the information, representations and advertising provided by or on behalf of the institution to those financial customers. Although not expressly mentioning the vulnerable customer it is clear that the regulator would like to see a more defined move away from a product centric approach to one that puts the customer's needs first.

The COVID pandemic has provided an example of just how critical it is to ensure that products remain relevant. Business interruption cover gave many clients a false sense of security (rightly or wrongly), believing that in the event of interruption to their business they would be covered. No one could have reasonably envisioned the extent of the current pandemic and not all business interruption policies included circumstances such as these in their contracts, leading to disillusioned customers and a social media frenzy. Ultimately in order to treat customers fairly under the circumstances we have to ask the uncomfortable question: are we prejudicing vulnerable customers by strictly relying on the legal provisions in their contracts?

Another critical component of ensuring appropriate outcomes for customers, is making sure that customers, especially those who are vulnerable, receive ongoing product communication. I have to wonder how many customers who were retrenched as a result of the pandemic relied on, or knew to rely on, their credit life insurance to meet their mortgage payments? Were they aware that this was an option that was available to them? When they signed for their home loan did they understand that this cover was included in the package?




## The strategic advantage of doing the right thing

And therein lies the upside, its not only about the warm and fuzzy feeling of doing the right thing. I have no doubt that a customer who is approached by his bank after being retrenched with an offer of a claim for credit life cover will be a customer for life. That is the strategic imperative of treating your customers fairly and that is where the importance of data comes in – knowing who your vulnerable customers are and what risks they face. Financial institutions have the numbers they just need to crunch them wisely. Lapse rates, repudiation stats, claims ratios, they all tell the story and identify your Conduct risks. High repudiation stats may indicate that customers are not informed about circumstances under which they may claim, they may have unrealistic expectations of the product performance due to misselling. On the other hand a product with very low claim rates, that happens to be sold as a bundled product may indicate that customers are not even aware that they have this benefit.

The 2019 Australian Royal Commission investigation into financial sector misconduct gave increased focus to the concept of vulnerable customers. This report highlights "that asymmetry of knowledge and power will always be present. Accordingly, there will always be a clear need for disadvantaged consumers to be able to access financial and legal assistance in order to be able to deal with disputes with financial services entities with some chance of equality." The challenge therefore is for financial institutions to make sure that no man is left behind.

## Key actions

— Information asymmetry is a major Conduct risk. This means that the financial institution has the advantage of having specialist knowledge about the product they are marketing, while the customer only has the knowledge they are given by the financial institution. To mitigate this risk, make sure that your customers have as much information as they need to make informed decisions

— Proactively manage the data you have and use this to identify Conduct risks where vulnerable customers may have been at risk

— Embrace a customer centric approach to business. Put the customer at the heart of everything you do and the product will sell itself


CUSTOMER
journey
Awareness
Consideration
Decision
Retention
Advocacy

KPMG

## Drivers

- How does governance at the corporate level foster organisational behaviour and root cause measures allowing business to deal with organised and financial crime. If the strategy is to divorce criminals from their financial and productive means, what culture do we foster to have that done?
- How do we collaborate across organisations, industries and the government and private sector divide? Walking together does the trick. How comprehensive and capable is the safety net we pull over the system
- Fundamentally, to make out for ourselves if we see compliance as a matter of business strategy, or do we have a culture of eradicating financial crime?

**Déan Friedman**
Partner
Forensic


# Financial Crime

## Chasing shadows of illicit events

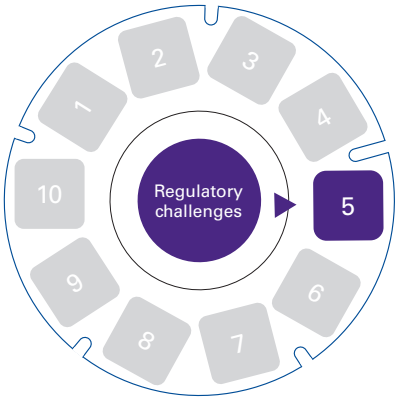
For many centuries the metal gold was considered a store of wealth and value and, because of its relative compactness to the value afforded it, an excellent way of moving such value or wealth. Gold is currently priced at approximately USD57 000 per kilogram. The price tag of pangolin scales varies between USD1 200 and USD3 000 per kilogram. A girl child goes for between USD2 and USD270 000, depending on the origin, destination and purpose of such person. Rhino horn goes for up to USD65 000 per kilogramme. Diamonds, for many years have been similarly considered such a store of wealth, or value. All the latter items are trafficked, which is illicit in nature. These activities are viewed and addressed based on smuggling, trafficking etc. All these value storage materials are however physical in nature, but also excellent means of transferring wealth between persons, irrespective of where they are. They are further either held in legal ownership or, in the case of human beings, illegal ownership concepts are applied to them.

One step further down the line is the concept underlying for instance hawalas, where wealth and value transfers on foot of the actions and honour of hawaladars, that is, the immaterial concepts of trust and confidence, to which is now attached a value. This is no different to the concepts of trust and confidence persisting in a functioning banking system, the difference being that, in a transactional banking system, there exists regulatory frameworks and rules that render events in what we refer to as the formal transactional banking system more visible and transparent. In the digital world the blockchain concept also gives a value to the concepts of trust and confidence, but in a different dimension than the formal transactional banking and hawala dimension. It is these levels of invisibility that attracts different purposes for these systems of value transfer, some of which are illicit, or simply visited with common law or statutory illegality.

There are many approaches towards mitigating or eliminating financial crime within the wider and somewhat bespoke definition thereof. Regulation and legal reporting obligations have mostly as an objective to make these crimes more transparent, but do not necessarily eradicate the scourge. Other approaches centre around education, thinking that awareness talks to the natural goodness of humans and so forth. Another, that the more we know of it will somehow deter threat actors. Much money goes into these initiatives. Yet another approach, driven by the basic concept of financial crime, which is the conversion of ill-gotten gain to the estate of a threat actor, suggests the best way to eradicate the scourge is by permanently separating the threat actor from the gain and the productive means needed for the gain. This entails legal and law enforcement action, supported by investigation.

This investigation effort is technically challenging given the material needed to work with and we found it more than often not strongly supported financially.

Whilst the latter approach is fraught with risk, particularly in respect of the less regulated dimensions where most financial crime occurs, it is seemingly the least funded and attended to environment in the fight against financial crime. Perhaps because it is mostly transactional, difficult to investigate and prosecute, fraught with physical danger to body and limb, and perhaps not desirable regarding the deployment of discretionary money within an environment where recognition towards the funding of such investigation and prosecution efforts are scant, if not of a high risk nature. The investigation effort however requires discipline, dedication and specifically sound trade craft.




The adage of following the money remains true when investigating financial crime. It is however much more convenient in a structured and regulated banking environment where the framework is compliant. Where the store of wealth or value used for the transfer thereof is a physical item the framework for the value transfer looks different. A rhino horn would for instance be layered as trash plastic, or grain, in a container on a ship. When the store of wealth or value is founded in the concepts of trust and confidence, the event of transfer is by means of a phone call, or a WhatsApp message. In the digital world it is by way of an inscription in a ledger protected by complex logical access control.

In some cases, these two universes, the one licit and the other illicit, may converge when wealth or value transfer is desired from the one to the other. That convergence leaves a hole in either one of the two universes or an unexplained gain in the other. These manifest for instance in the form of a company receiving income from sources not explained by its business. There are many more complicated ways of doing this. The financial crime investigator thus often needs to search for that of which evidence is not there, or an explanation that does not follow logically, much like an analyst of an overhead photograph will search for a shadow to determine the existence of a physical structure photographed.

Profiling as an investigation technique is both subject to criticism and fraught with completeness risk, particularly financial profiling, but it remains a manner of identifying the shadows of events destined to be hidden away from the licit eye. When you want to work out if cash handling persists financial profiling helps identifying obligations not covered by licit flows, as an example, or a company that cannot be found in a complex transaction string.

A computer profile does not evidence transactions the user does not want to make visible, but it does reflect the existence of artefacts consistent with for instance layering or the use of a certain value transfer technique, or inconsistent for instance with the published use of the computer. Anti-forensic techniques used in cybercrime removes the evidence of the event, but often leaves shadows in the form of forgotten or neglected artefacts.

Not only evidence, but also intelligence, helps to build the many views of facts and events we are led to believe exist.

We believe that the many views that can be built discloses the shadows of illicit events, when overlaid with each other, enabling effective factual scenario building. The tradecraft often requires a novel and innovative approach. Equally, the constitution of such work, the participants thereto and the funding thereof also requires novel and innovative approaches.

## Key actions

— Have a view of the predicate crimes and issues driving the money laundering aspect of financial crime. Recently in SA it was the state capture concept. International Wildlife Trade is currently a major focus point predicate to financial crime. But do we have a view of drugs, human trafficking, soft and hard commodities? Coming soon is climate change related predicates. More ideal and logically derived concepts obtain value and becomes tradeable. Pandemics like COVID create predicates. They all converge at the organised crime level, casting its shadows in the licit transactional environment-can we see those shadows?

— Do we have a deep understanding of the attributes of our organisation making us attractive to financial crime threat actors, and what is to be done about it?

— Where the illicit application of trust and confidence finds use in the licit structures of trust and confidence, like a bank or mobile services provider, the licit and illicit attributes become difficult to distinguish and identify individually for what it is. Are we able to do this consistently?

KPMG

## Drivers

- The evolving data privacy regulatory landscape is transforming the way organisations and individuals think about the use and protection of personal information
- The continued sophistication of cyber-crime is putting a focus on security for privacy within organisations
- Increased public awareness and concern regarding the collection and use of personal information is driving privacy compliance

**Beulah Simpson**
Senior Manager
KPMG Privacy Practice

# Data Privacy

## Protecting your data as the asset that it is

For some time we found ourselves commenting on the comparably embryonic state of our privacy legislation in comparison to jurisdictions like Europe where the GDPR has been effective for some time. After the 7-years hiatus, the Protection of Personal Information Act ("POPIA") finally came into effect on 1 July 2020 and will be enforceable from 1 July 2021. This marks a key milestone in South Africa's privacy regulatory journey – one that will change the way that organisations think about and process personal information in its day to day business activities. Businesses now have less than 6 months (from the writing of this article) to become fully compliant with POPIA. However, with a sound plan and enough determination – it can be done.

## Privacy Challenges of 2021

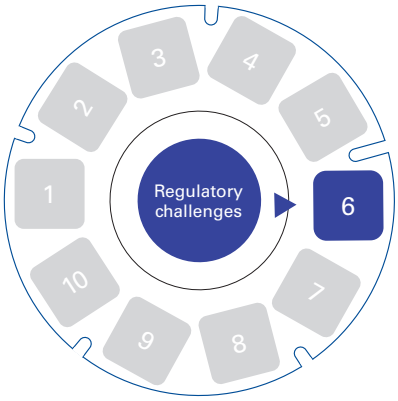
The biggest privacy challenge many organisations are facing is determining where to start with their POPIA compliance journey. Having performed numerous POPIA readiness assessments we can say that each organisation's privacy compliance challenges and priorities differ. However, we have set out below what we consider to be the top 5 of the POPIA challenges that stand out to us:

### Non-existent or poor privacy governance structure

Too often, when we perform a privacy maturity assessment, we find that there isn't a clear privacy governance structure and/or that roles and responsibilities for privacy have not been assigned to employees. A strong privacy governance structure is essential to comply with POPIA. After all, the first condition of POPIA is "accountability" (as set out in section 8 of POPIA) and requires that organisations ensure that all eight conditions of POPIA are complied with and that "all measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself". This is an impossible task without the right privacy governance structure embedded within the organisation.

### Interpreting and applying POPIA principles in the age of AI and machine learning

More and more organisations are exploring how they can deploy AI tools to generate greater value from the personal information they have gathered over the years. However, documentaries such as The Social Dilemma are putting AI and the organisations that use them in the spotlight. With increased consumer awareness and regulatory pressure, organisations have no choice but to navigate the use of AI in a privacy-compliant manner. POPIA, and the regulations and guidelines currently published thereunder, do not expressly address the questions that many organisations will have about the privacy-compliant use of AI. Instead, organisations will need to




interpret the principles-based legislation to make sense of this challenge itself, including conditions governing "collection of personal information for a specific purpose" (section 13), "further processing to be compatible with purpose of collection" (section 15), "minimality" (section 10), "notification to provided to the data subject when collecting personal information" (section 18) as well as consent/lawful justification (section 11).

**Failing to identify the risk when using a third party to process personal information**

Often, for convenience or efficiency, organisations ("Responsible Parties") outsource services which incidentally or intentionally involve the processing of personal information (for example, engaging with financial services intermediaries or outsourcing actuarial functions, documentation archiving, cloud-storage, performing criminal checks on prospective employees or delivery services). When organisations rely on third parties (referred to as "Operators" in POPIA), there may be an expectation that the same level of privacy controls will be applied by the Operator as those applied by the Responsible Party. However, this is an area that is not always sufficiently considered, vetted or audited - until there is a serious data breach of course. This poses a key risk to organisations which is often not adequately catered for within the privacy control framework.

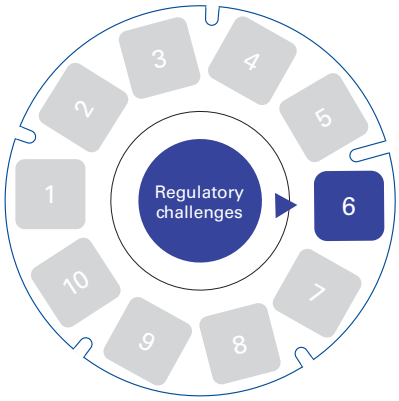
**Organisations underestimate data subject access requests**

Many organisations have completely underestimated the privacy risks and administrative burden associated with data subject participation. The numerous rights of data subjects are summarised in section 5 of POPIA and requires organisations to take decisive action. In our experience, many organisations tend to manage their data subject access requests on an ad hoc basis, with no centralised or formalised process to ensure that the organisation is able to respond fully, timeously or appropriately to a data subject request. This may prove to be particularly troublesome for organisations with data sprawl (i.e. when personal information is widely dispersed across an organisation).

**Policies, procedures and controls are not enough**

While organisations should design and implement policies and procedures to ensure that its processing activities are POPIA-compliant and satisfactorily cater for privacy rights and obligations, policies and procedures, alone, will not be sufficient. Many organisations have been focusing all their efforts on policy drafting instead of nurturing a privacy culture where employees are aware and understand their responsibilities when dealing with personal information and are empowered to action those responsibilities. Compliance can never be achieved if employees don't buy into the importance of POPIA within the organisation or don't understand how to apply privacy principles to their day to day business activities.

> "Too often, when we perform a privacy maturity assessment, we find that there isn't a clear privacy governance structure and/or that roles and responsibilities for privacy have not been assigned to employees."
>
> Beulah Simpson




## Key actions

— **You don't know what you don't know** – every big project requires a sound project plan. Every organisation should consider starting their POPIA compliance journeys (if they have not done so already) with a POPIA Gap Assessment to establish the organisation's existing privacy controls and to identify its POPIA gaps. This will assist the organisation in prioritising the actions required to comply with POPIA and to allocate the necessary resources to be compliant by 1 July 2021

— **Establish an appropriate governance structure** - Ultimately, the privacy governance structure must be one that is appropriate, having regard to the organisation and must be effective for identifying, assessing, monitoring and reporting on privacy related risks and breaches through the governance structures. It must include the appointment and registration of an Information Officer but may also include appointing deputy information officer or establishing privacy committees, forums or teams. It is also important that roles and responsibilities filter down the chain of command and that each employee understands their privacy obligations

— **Recognise when you need professional assistance** – Each organisation is encouraged to use their internal resources to drive POPIA compliance, however, it is important that these internal role-players have a clear understanding of what this means practically. When it comes to interpreting and applying POPIA – many organisations may need to seek professional advice in order to drive POPIA compliance within their organisation (particularly when it comes to more complex processing activities such as those involving AI, robotics, machine-learning, automated decision making)

— **Don't overlook the risk posed by third parties** – Third parties pose one of the greatest privacy risks (depending on who that third party is of course). It is important that organisations enhance their procurement processes to include privacy due diligences in respect of third party suppliers (Operators), include robust privacy clauses in their third party agreements and perform privacy audits, particularly in respect of high-risk Operators

— **Consider technology enablement** – it is important to keep abreast of privacy technology developments and to consider how technology can be deployed to support your organisation with POPIA compliance. For example – is there a technology solution that can assist you in automating data subject access requests and, if so, does it make commercial sense having regard to the number of data subject requests and complexity of each request? This is an area that all organisations should keep in mind in 2021 and beyond

— **Prioritise cultivating a privacy culture** – For privacy to become embedded in an organisation, it is important for organisations to cultivate a privacy culture – one of the ways this can be achieved is by establishing a privacy training and awareness programme which should be revised annually to remain relevant to employees

KPMG

## Drivers

- Insurers' capital has weathered the Covid storm well
- Experience has shown that legal risk can create capital strain
- The actions of insurers are increasingly judged by the court of public opinion through social media

**Derek Vice**
Partner
Financial Services Audit

# Capital & Liquidity

## Balancing inherent tensions to weather the storm

### Insurance Capital in 2021

Capital. The word Capital has multiple and varied meanings. It can mean:

- the principal or most important (the capital city);
- involving the death penalty (a capital offence);
- very serious or fatal (a capital error);
- the chief town or city (South Africa's capital is…);
- a capital letter;
- the top of a pillar;
- wealth or property that is used or invested to produce more wealth (investment capital, capital goods, the capital sum); and
- importantly, the root of capitalism.

You can capitalise, be a capitalist, capitulate and even decapitate. Clearly capital is important.

A common thread between these is that they are connected to the essence, or life, of something. The capital of a country was historically the centre of the government and often the economic hub. A capital offence is so serious it can cost one's life. The start up capital is the life blood of an entity. And it is fair to say, the capital markets are the lifeblood of capitalist systems around the world.

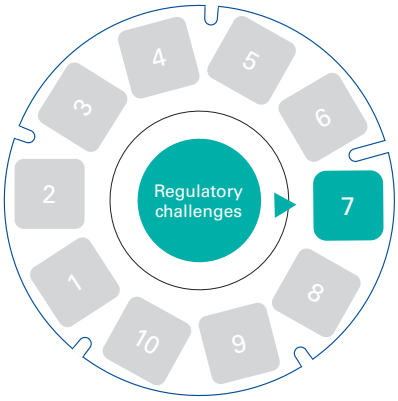
However, in financial services, notably banking and insurance, the word capital has taken on a specific regulatory meaning. It is not simply the initial investment that launched the enterprise. In many instances, the regulatory capital amount is multiples of this initial investment. Although legally prescribed (through complex formulae and ratios), the amount of the capital requirement attempts to represent the amount of excess assets these entities must hold to remain solvent in stressed scenarios. These stressed scenarios are usually expressed in terms of an extreme event (a one in two-hundred-year event), or a confidence level (like a 99.5% confidence level[1]). Regulatory capital is often expressed as a ratio. A capital coverage ratio of 2.0 would suggest that the entity is holding double the required amount[2].

By prescribing a capital amount, regulators are trying to address one of the inherent tensions in the capitalist model. This is the tension between an investor's required returns and the protection of consumers and beneficiaries of financial products. Without the regulatory capital buffer, directors might be encouraged to declare dividends to a point at which a few unfortunate events could make the entity insolvent. In contrast, an excessive capital requirement stifles business and drives away investments by reducing investors return on their capital.

It should be noted that failing to meet the regulatory capital requirement is, in certain circumstances, a figurative "capital offence." Consistent failure to meet regulatory capital requirements can see an entity closed to new business or even put into liquidation. Hence companies tend to be cautious in meeting these requirements.

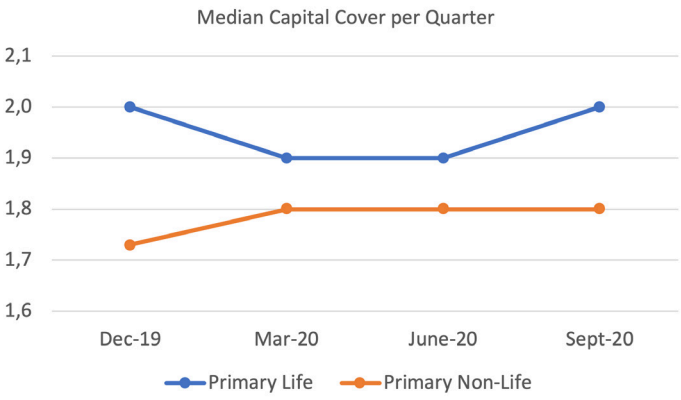
1 Which itself means that in 99.5% of scenarios we would expect the entity to remain solvent.

2 Put simply, if the regulatory assets are 100 and the regulatory liabilities are 80, then the excess is 20. If the capital requirement was 10, the capital cover would be 2 times. If the capital requirement was 5, the capital cover would be 4 times.




*2020 provided a real-world test case of the appropriateness of regulatory capital cover for financial institutions in South Africa* (and internationally). The Covid pandemic represents the sort of unexpected events which the regulators are trying to protect consumers and beneficiaries against.

**Insurers' capital cover from December 2019 to September 2020 showed the following trend[3].**




This is supported by the results of the listed life companies, which showed solvency cover ratios between 1.82 and 1.87[4] without significant variance from the prior year. This was in the context of R8.251 billion of Covid specific provisions raised by these companies[5]. And, on the non-life side, apart from business interruption claims, the generally positive impact from lockdown on claims experience.

Essentially, life insurers experienced a 5% reduction in cover through the middle of the year, with a rebound by September. Although several factors contribute to this it clearly shows an overall level of resilience in the insurance industry. Whilst profitability has been negatively impacted, the short-term impact of this on solvency has been muted.

The relative stability of the capital numbers over the period is probably intentional. Insurers maintain a target cover ratio and declare excess as dividends.

One of the tools to maintaining solvency during Covid has been a moratorium on dividends. At least amongst the listed entities, we know that dividends were withheld, which would offset the abovementioned increase in the provisions and reduced profits.

This raises the question: *is the insurance industry over-capitalised?* With capital significantly more than the regulatory requirement, could there be an argument to release some of this to shareholders? Although in early 2021, this would be rash and impulsive; once/if the year settles and the vaccines help bring Covid under control, this could be a debate worth engaging. This might even be a requirement as investors start seeking returns in a post-Covid world.

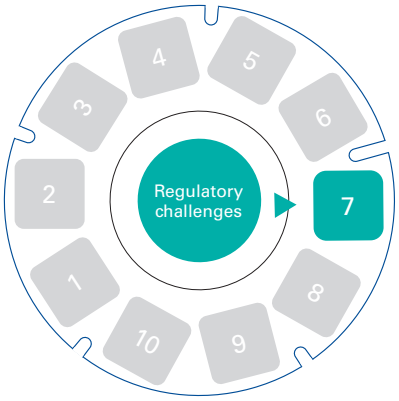
It is important to note that the regulatory capital cover could be at these levels because the insurers are intending to use this excess (i.e. it is not simply held to meet a regulatory requirement). It is seldom the case that this excess is under-utilised. Quite the contrary, many insurers are investing heavily into new ventures, system upgrades, digitisation and managing their asset allocation to maximise returns on this capital. Often these funds are ear-marked as "start-up" capital to launch new ventures. The excess could also be at these levels because the insurers have their own view of capital, which is to say they allow for aspects not included in the standard/prescribed capital models.

An interesting impact of this regulatory capital position was that many insurers were able to make morally significant contributions to Covid relief. From premium holidays, to direct contributions to Covid funds, the insurance industry showed its moral fibre and supported its customers in various direct and indirect ways. In considering the quantum of capital cover, directors might want to consider whether a portion of this cover remains committed specifically for such scenarios. Insurers could maintain a similar level with the knowledge that 0.1 of that cover is specifically designated to provide customer support in a catastrophe scenario (assuming such cover is not directly required).

[3] Based on the "Selected South African insurance data" prepared by the Prudential Authority on a quarterly basis. These amounts represent the median position of the primary life and non-life industries.

[4] Based on their June year end/half year results: Sanlam 1.87; Old Mutual 1.82; MMI 1.85; Discovery 1.83; and Liberty 1.82.

[5] Based on their June year end/half year results: Sanlam had a pre-existing pandemic provision; Old Mutual 2.793bn; MMI R983m; Discovery R2.3bn; and Liberty R2.175bn




> 2020 provided a real-world test case of the appropriateness of regulatory capital cover for financial institutions in South Africa.
>
> Derek Vice

This would turn what has been a random act of kindness into a policy decision to utilise the business to provide support in the worst times. In an age of ethical investing and corporate social responsibility such "*moral capital*" might even become a distinguishing feature of reporting entities.

One of the challenges for non-life insurers has been getting to grips with the confusing interaction of lockdown with business interruption clauses. This has highlighted two aspects which are not directly covered in the standard formula[6].

The one is the importance and potential impact of reputation. Reputation has often been considered by entities as part of their own solvency assessment. The more nuanced aspects seen during the pandemic is impact of the court of public opinion. Whilst reputational risk is linked to a specific brand, the court of public opinion rules on groundswells, hashtags, and trending views. It can create significant pressure, especially in times of stress. The risk to capital is that any brand associated with this hashtag or trending view can then be scoped into the court's ruling. The question it raises is *how does one allow for the vagaries of the court of public opinion in considering an own view of capital?*

The other aspect was the impact of legal risk. Whilst legal risk might fall under the broad heading of operational risk, what the business interruption debate has shown is that a few changes to policy wording can, under stressed scenarios, have a significant impact on an entities capital (or expected behaviour). The question this raises is, *are there policy wordings and interpretations, which create legal risk that should be allowed for in one's own solvency assessment?*

Given the limited allowance for, and quantification of, these risks under the standard regulatory capital requirements, we can expect to see more bespoke considerations of these in 2021. We also expect ongoing dialogue from the regulator to understand such exposures.

Capital is principal and most important to insurers. Failure to meet regulatory capital requirements could be a symbolic capital offence for insurance entities. Failure to allow for known, emerging or possible risks in one's own solvency assessment could be a very serious or even fatal error. However, if capital remains on top of the pillars of the organisation, it is wealth that can produce more wealth and support the capital markets.

## Key actions

— Does our experience of Covid change our own view of our capital requirements?

— Which vague policy wordings could be attacked in future catastrophes?

— Is discretionary support for customers in times of stress not actually a moral imperative?

[6] The standard calculation used to calculate regulatory capital for insurers in South Africa.

KPMG

## Drivers

- Regulators are increasingly embracing innovation. Countries such as China are taking the lead in development of CBDC, which could further challenge the dollar's reserve currency status
- Growing public awareness and interest in digital assets (including crypto currencies and stable coins) given the various benefits of using digital assets
- The announcement of the impending launch of Facebook's Libra token (renamed to Diem) in 2019, which poses a threat to traditional fiat currencies given the size of Facebook's userbase
- Challenging global conditions due to COVID-19 have accelerated various digital adoptions by many years, this is also true for digital currencies

**Rudi Sturm**
Associate Director
FRM Credit and Capital Risk

# Central Bank Digital Currency

## The evolution rather than revolution of fiat currencies

Central Bank Digital Currency (CBDC) is effectively a type of crypto asset representing the digital form of the fiat currency of a specific country, backed by the country's central bank. CBDC attempts to incorporate all the advantages of Distributed Ledger Technology (DLT) while ensuring that the central bank retains control of the currency, particularly to allow the continued application of monetary policy and relevant regulation.

There are two main forms of CBDC currently being proposed, namely a 'retail CBDC' which would be used like a digital form of the fiat currency by people and companies and a 'wholesale CBDC' which would be used only by permitted institutions as a settlement asset in the interbank market and for international payments.

The adoption of an alternative currency and payment system in the form of CBDCs seems to be inevitable based on increased digitalisation, which has accelerated due to lockdown restrictions and the continued rise in popularity and functionality of crypto currencies and platforms. This is further driven by the potential of CBDC to address challenges and concerns relating to:

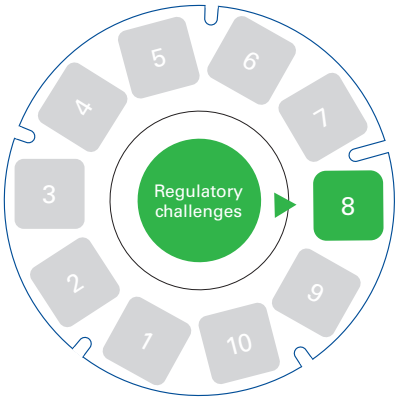
- Inefficiency in current payment systems;
- Need for improved data collection and information trails for central banks and tax authorities; and
- Promotion of greater financial inclusion.

In a survey released in January 2020, the Bank for International Settlements (BIS), asked 66 central banks whether they are working on a CBDC; 80% of these central banks confirmed they are exploring the idea, while 10% are "imminently close" to launching a CBDC to the general public. The BIS further noted (in working paper no 880: Rise of the central bank digital currencies: drivers, approaches and technologies) that that higher mobile phone usage (a measure of an economy's overall digitisation) and higher innovation capacity are positively associated with the likelihood that a country is currently researching or developing a CBDC. Retail CBDCs are more likely to be developed where there is a larger informal economy, and wholesale CBDCs are more advanced in economies that have higher financial development.

Based on the extensive research and development performed and given the perceived benefits of using CBDCs, the implementation of CBDCs seems to be a question of "when" and "how" as opposed to "if".

## "How" to implement

The below highlights some of the key aspects of implementation that need to be considered and it is recommended that decisions relating to the below design elements are made by central banks in partnership with local banks (and other financial institutions) along with input from DLT technology platforms and companies (e.g. 2nd and 3rd generation blockchain platform projects like Ethereum, Cardano, EOS and Polkadot).




There are four attributes of CBDC technical designs noted by the BIS, based on the taxonomy of Auer and Böhme (2020).

— The first and foundational design choice is the **architecture**, that is which operational role the central bank and private intermediaries take on in a CBDC.

— The second technical design choice relates to the **infrastructure**. The infrastructure can be based on a conventional centralised database or on DLT. It is important that a CBDC is secure from outages at the central bank.

— The third design choice concerns how consumers can **access** the CBDC. Account-based CBDCs are tied to an identity scheme, which can serve as the basis for well-functioning payments which are easier to regulate. An alternative is to base access on so-called digital tokens which represent the currency.

— Closely tied to the domestic access framework is the fourth design choice, whether CBDC will be used for **cross-border payments**, which relates to the retail and wholesale interlinkages in a CBDC's design and its accessibility to non-residents.

There are a rising number of central banks which are considering "Hybrid" or "Intermediated" architectures where the CBDC is a cash-like direct claim on the central bank, but the private sector manages customer-facing activity. Only a small number of jurisdictions are considering designs in which the central bank takes on an important operational role in the customer-facing side of payments.

Whereas many central banks are considering multiple technological options simultaneously, current proof-of-concepts tend to be based on distributed ledger technology (DLT) rather than a conventional technological infrastructure. Nevertheless, access frameworks tend to be based on account identification rather than allowing for token-based fully anonymous access. Most CBDC projects have a domestic focus.

## Challenges

The key challenges that are often noted when CBDCs are considered, relate to:

— **Security.** CBDCs potentially present an even larger attack threat (especially if not sufficiently decentralised by utilising an indirect architecture) and could be more likely to be subjected to cyber-attacks given that in theory there is now one centralised point of failure.

— **Scalability.** It has not been conclusively proven that DLT could be scaled sufficiently to incorporate large numbers of transactions. If this is fully implemented, there may still be question marks on the resilience of the technology.

— **Digital infrastructure dependence.** Based on research from the BIS, jurisdictions with greater mobile phone use and/or internet use may have a more developed infrastructure for the central bank to develop CBDCs. Therefore, less developed countries could be left behind.

## Way forward

Given the pace of advancement in DLT technology in the private sector which is enabling banking like services to customers outside of the formal financial services sector, regulators and banks alike are left with no choice but to adapt or run the risk of becoming less relevant.

However, the transition to CBDCs is expected to be gradual given the new and unfamiliar nature of the technology, unproven scalability and elevated risk posed by a hasty implementation. CBDC implementation is expected to run in parallel with traditional forms of currency and is currently seen as complimentary to the current financial system as opposed to a replacement of traditional currencies and services.

As banks traditionally provide many of the services that CBDCs are aimed at enhancing, banks are expected to play a large part in this evolution in partnership with central banks, to design a solution that is fit for purpose for a particular country, based on the economic advancement and the maturity of the country's financial system.

## Definitions

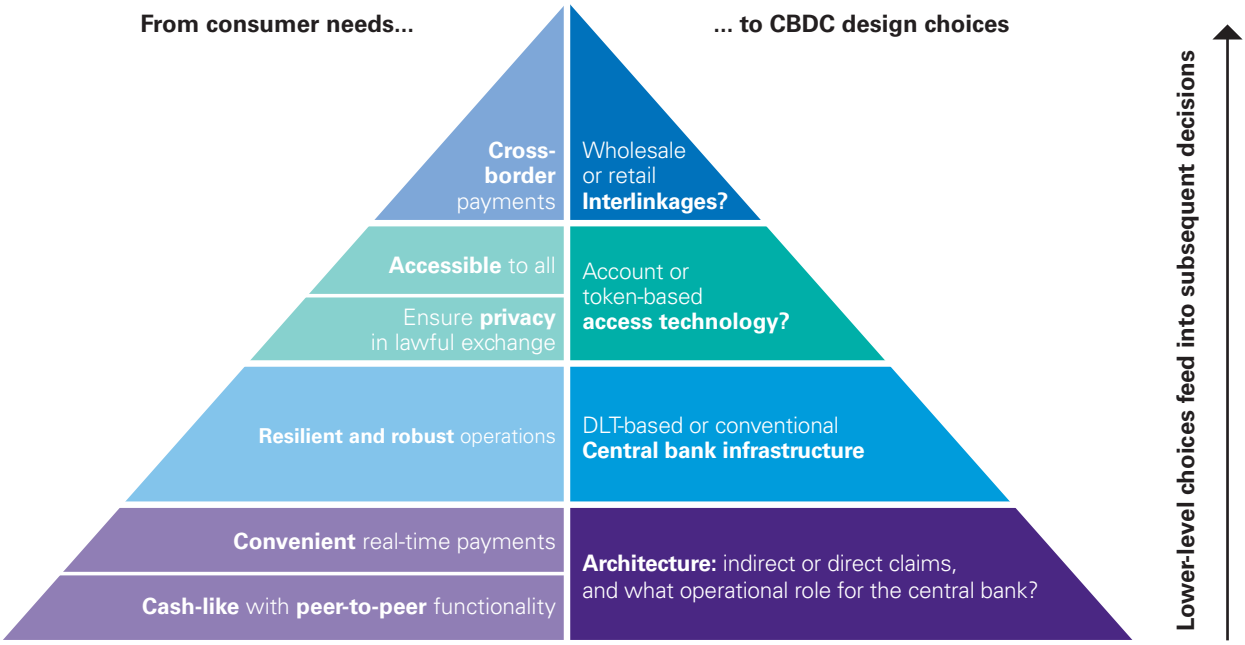
**Distributed ledger technology (DLT)** is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. DLT is a decentralised database managed by multiple participants, across multiple nodes. Blockchain is a type of DLT where transactions are recorded with an immutable cryptographic signature called a hash. (https://www.r3.com)

**A crypto asset is a type of DLT** and is a digital representation of value that is not issued by a central bank, but traded, transferred or stored electronically by natural or legal persons used for the purpose of payment, investment or other form of utility for the user. (SARB) Crypto currencies like Bitcoin are one type of crypto asset. Assets like Bitcoin are not truly currencies yet. They can be units of account, but hey are not yet a store of value or a medium of exchange to be a full-fledged currency. There are many other types of crypto assets, such as stable coins, security tokens and utility tokens.

**A stable coin** is a privately (i.e. non-central bank) issued crypto currency with a stability mechanism incorporated into its design with the aim of closely mimicking the value of (i) a single sovereign currency; (ii) a basket of sovereign currencies; or (iii) another reference asset such as a commodity or even another crypto asset. (SARB).

**A central bank digital currency** (CBDC) is essentially digital cash which uses a blockchain-based token to represent the digital form of a fiat currency of a particular nation. (www.investopedia.com)

## Illustration relating to "how" to implement [1]




The CBDC pyramid maps consumer needs onto the associated design choices for the central bank, The left-hand side of the CBDC pyramid sets out the consumer needs and associated features that would make a CBDC useful. The pyramid's right-hand side lays out the associated trade-off - forming a hierarchy in which the lower layers represent design choices that feed into subsequent, higher-level decisions.

Source: Auer and Böhme (2020).

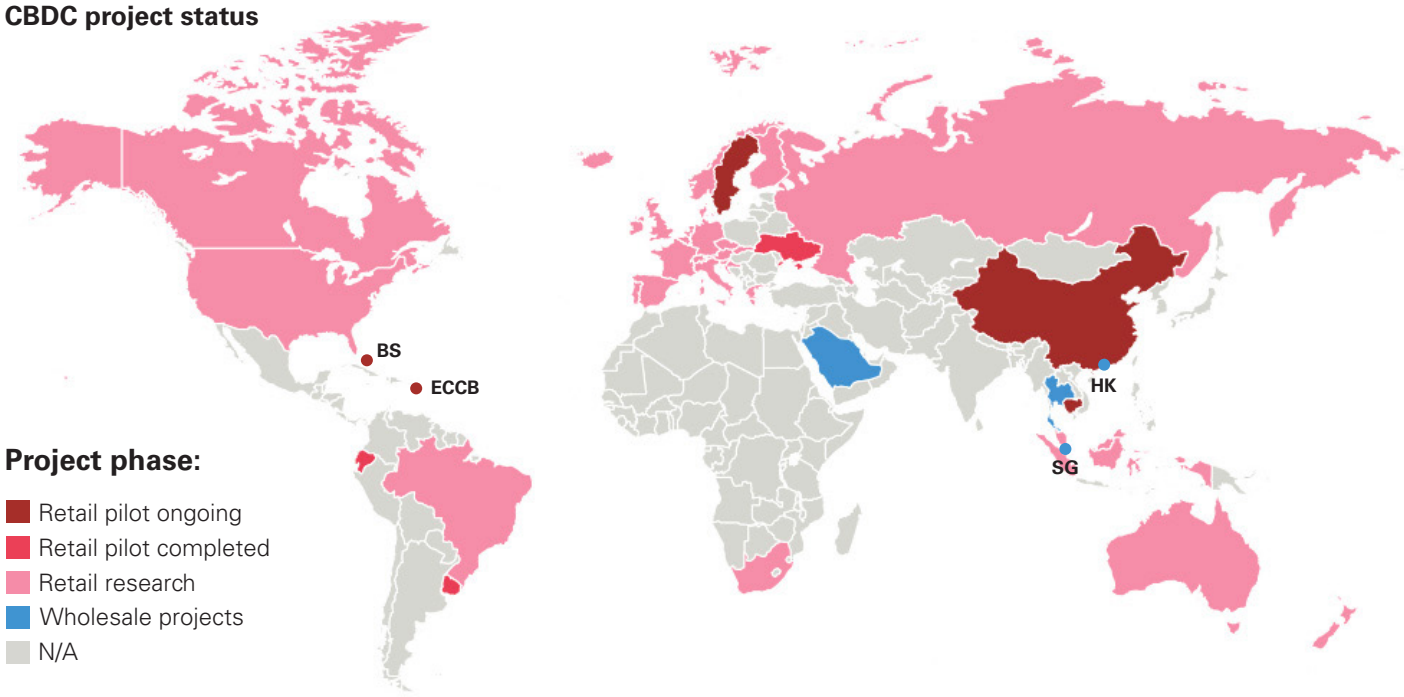
## Key actions

— Financial services institutions should develop a comprehensive understanding of CBDC, digital currencies and other decentralised finance applications (DeFi), particularly at an executive level. This could entail creating digital asset leads and teams, performing research and participation in collaborative research projects locally and internationally

— Given the experience of banks as intermediaries, significant customer bases and broad IT and financial skills, it is likely that a large part of the design and implementation will be driven by existing financial institutions and leading crypto companies, in partnership with central banks

— Central banks can learn from one another, other banks or financial institutions, the BIS, the WEF and other stakeholders by sharing information relating to drivers, approaches and technologies

## Illustration relating to Evolution rather than revolution of fiat currencies paragraph [2]




BS = The Bahamas; ECCB Eastern Caribbean central bank; HK = Hong Kong SAR; SG = Singapore.

The use of this map does not constitute, and should not be construed as constituting, an expression of a position by the BIS regarding the legal status of, or sovereignty of any territory or its authorities, to the delimitation of international frontiers and boundaries and/or to the name and designation of any territory, city or area. Source: central banks' websites.

[1] BIS working paper no 880: Rise of the central bank digital currencies: drivers, approaches and technologies

[2] BIS working paper no 880: Rise of the central bank digital currencies: drivers, approaches and technologies

KPMG

## Drivers

— Organisations are overwhelmed with an unprecedented influx of digital solutions as they try to prioritise operations in the "new normal" leaving them vulnerable to cyber attacks from unexpected sources

— Trust has become an important commodity and reputation is not something organisations want to risk

— It's a matter of "when" and not "if" as the cyber threat landscape evolves

**Marcelo Vieira**
Partner
Cyber Security

# Cyber

## Protecting the lifeblood of the organisation

COVID-19 triggered the survival instincts of businesses, who have accelerated their digitisation to succeed in the new reality. The idea that data has become the lifeblood of the organisation has been reinforced as boards seek to harness the potential of our digital economy, create new customer experiences, transform their services, and drive efficiencies and cost savings in the wake of the pandemic. The future is being created from a fusion of new business models, new technologies, and new partnerships.

In this changing world, there are ruthless entrepreneurs who are making money in this new economy. Unfortunately, they are cyber criminals and they are on the wrong side of the law. They pose new challenges to legitimate businesses, and companies need to think differently about how to protect their competitive advantage and develop new models with a goal of becoming and remaining cyber secure. Cyber security professionals need to demonstrate they can protect the heart of the transformed business with an agility of thought and action that recognizes the pace and speed at which cyber criminals operate. They need to assemble the kind of collaborative talent — across the enterprise — that is able to take a proactive stance and meet these issues head on. The CISO can't do it all. New partnerships are needed, technology is an opportunity, not a threat, and cyber security is becoming a key business enabler.

Given the risks the world currently faces, we have picked some cyber considerations that will likely shape or impact the way organisations approach security in the next year or so.

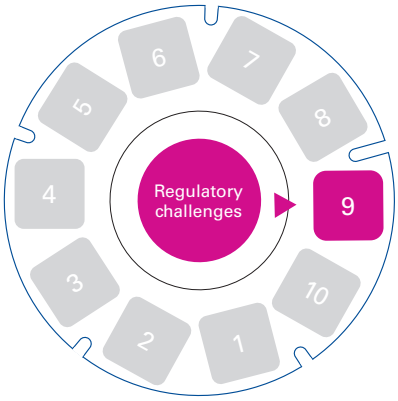
### The digital race

As the world continues to operate under the so called "new normal", organisations within the financial services sector are overwhelmed with an unprecedent influx of digital solutions in order to prioritise operations[1]. The shift towards a digital workforce has seen organisations invest heavily in digital infrastructure to enable inter-connectivity without physical presence, but this mass adoption of digital technology has exposed organisations to additional risks. The 2020 World Economic Forum report expects cyber attacks to increase by 75% in the short term, given the context of the new normal.

Besides the drive towards a digital workforce, cloud adoption was significantly fast tracked over the past year. Historically, IT has been responsible for infrastructure provisioning, and, before the cloud, was primarily focused on the challenges on the ground (pun intended). The security team is charged with scanning that infrastructure for vulnerabilities, but they often don't know what to scan because there often is a disconnect with IT on an updated threat list. Managing infrastructure and the related assets has always been demanding, but in the cloud, where everything is faster and more ephemeral, getting security involved early and hardcoded into the provisioning plan is a challenge many companies are struggling with.

In terms of the cloud, across multiple industries, the CISO's organisation is largely not prepared to enable the business, neither in terms of skills nor talent. In the cloud, the priority is information protection. What we're finding more and more is that the way data is being deployed in the cloud is often not necessarily resilient. We're not simply talking about multiple availability zones,

[1] https://www.soprabanking.com/insights/how-banks-are-using-technology-to-combat-covid-19/




but the ability to recover critical assets if there's a major breach.

## Regulatory wave

Thousands of attacks are launched each day targeting the financial service operators and customers need assurance and trust that their Personally Identifiable Information (PII), and transactions are kept secure. This trust is priceless.[2] The regulators have also realised the importance of securing customer data and we have seen new regulations and guidelines being announced more frequently. At the same time organisations need to maintain confidentiality, integrity and availability of its critical business functions.

Many organisations may have to shift their focus to the Protection of Personal Information Act (POPIA) and the requirements thereof in order to meet the 30th of June 2021 deadline.

Lastly, with the increased regulatory pressures and increase of the level of risk, it is becoming evident that organisations must not only consider the risks from within their organisation but also from those introduced by their own third parties. A lack of alignment between two parties may render controls enforced by an organisation obsolete. It is becoming increasingly essential to understand the significance of third-party risk management.

## Adoption of technology

The South African government requires employers to provide and maintain a safe working environment. The promise of an effective vaccine rollout will see a split working arrangement being implemented by organisations, with the pros and cons of working from home now being fully understood. Organisations are likely to use technological improvements to help them enhance workplace safety and productivity. As technology is adopted to combat the risks of COVID-19, organisations should also revisit their risk identification processes when deploying new digital services in their businesses.

We foresee a greater emphasis on collaborative technology in the smaller working areas such as pods and small meeting rooms. Risk identification processes should ensure that secure online collaboration is taken into consideration, by verifying that the platform is securely built from the foundation and is maintained by its thoroughly vetted third party suppliers.

## Incident Detection and Response

Whilst detection and defence against cyber-attacks is important, organisations must prepare for worst case scenarios. Companies in the financial sector have started to ask the question "what happens if we experience a cyber incident?".

The answer to this question lies with both the ability to detect and respond to a cyber incident. A recent report conducted by researchers Ponemon established that the global average for an organisation to identify a data breach is an unbelievable 177 days with a further 56 days to contain the breach.[3] With an evolving cyber threat landscape, there is high risk that these cyber incidence response times will increase if organisations are not fully prepared.

Through the introduction of the KPMG Digital Signals Insights Platform, we have seen the collation and interpretation of data aide organisations in understanding their key cyber threats through the monitoring of social media, the dark web, leaked databases and a multitude of other vectors. Fully exercised cyber incidence response plans that detail how an organisation will detect, respond to and recover from cyber incidents have become a prerequisite for financial institutes who wish to mitigate the effects of a data breach or cyber incident timeously.

## Cyber Insurance

A number of organisations are finding options to transfer their risk. As such, there has been an increased uptake of cyber (risk) insurance. Whilst, insurers will conduct their own assessments, the organisation needs to play their part in protecting its critical business functions, assets, data, and resources. Most importantly, organisations should be cognisant of the fact that cyber (risk) insurance is not a silver bullet. There are costs that their cyber (risk) insurance policy will not cover such as reputational damage, and incidents which originate from third parties.[4] Cyber (risk) insurance should complement the overall cyber risk management plan.[5]

2 https://www2.deloitte.com/global/en/pages/risk/articles/cyber-risk-financial-services-industry.html

3 https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

4 https://www.coalitioninc.com/blog/10-costs-your-cyber-insurance-policy-may-not-cover-unless-its-with-coalition

5 https://www.information-age.com/cyber-insurance-123474579/#:~:text=Typically%2C%20cyber%20insurance%20policies%20provide,the%20failure%20to%20safeguard%20data.

## A forward-looking view

— **Board Reporting**

Understandably, shareholders and directors are increasingly concerned about cyber security incidents. Leadership needs to ensure that cyber security is an integral component of the executive's role in risk oversight.[6] Cyber security concerns should be communicated by cyber professionals in a business language that executives can understand. This can involve illustrating and communicating cyber risk management awareness solutions in business context e.g. using Data & Analytics to understand prevalent threats and projecting these using simplistic dashboards (through use of tools such as PowerBI, Tableau and other leading tools.

— **Targeted training and awareness**

Despite the use of innovative technology and increased security, the weak link in the cyber security defences and source of many security breaches remains human error. Cyber criminals commonly use social engineering techniques to breach organisations with the sector. As such, there should be increased focus on security awareness training and developing user (and targeted) awareness campaigns which incorporate contemporary threats.

— **AI and Machine Learning**

A KPMG survey conducted in 2020 concluded that 87% of organisations report that Artificial Intelligence (AI)/ Machine Learning (ML) capabilities are a "must-have" for cloud and new security purchases. With the lack of available cyber skills within Southern Africa and globally, organisations have turned to AI to plug the skillset gap. Organisations need to respond to the increase in complexity and sophistication of cyber-attacks. Mitigating actions to address these complex cyber risks need to be taken. Consideration should be given to AI/ ML as an aide to addressing these risks. AI aims to eliminate the risk of human error whilst ensuring that an organisation's IT landscape is constantly monitored for sophisticated attacks that may evade standard detection techniques.

— **Cloud Adoption**

Work to understand — and communicate to the entire enterprise — the connection between business enablement, business resilience, and information protection. It's not much of a departure from how you would do it on premises, but it's a little bit different when you've got critical data across regions in the cloud. Making this part of your DNA enables you to weed out the "noise" from an operations perspective so you can focus on the bigger security priorities.

Moving past 2020 and progressing to 2021, organisations within this sector should ensure that a top-down approach is followed for endorsing all cyber security initiatives and held accountable for the success of cyber security objectives. Furthermore, organisations should take a collaborative approach to tackling cyber related issues by encouraging cyber accountability across the organisation. A cyber resilient aware organisation has become increasingly important as cyber-attacks against the financial sector will continue to rise.

## Key actions

— Human error remains one of the biggest weakness in any cyber risk management plan.[7] An effective and targeted security training and awareness program is the only way to change user behaviour and reduce this risk. Educating all employees will develop a strong cyber security culture thus yielding the best return

— Encouraging cyber accountability across the organisation

— Embedding the responsibilities of cyber security, as well as the role of the CISO, in the first line of defense — preferably formally — and link these tasks to annual performance targets

6 White paper " Reporting Cybersecurity Risk to the Board of Directors" by ISACA
7 https://www.globalservices.bt.com/en/insights/blogs/cyber-security-trends-in-financial-services-for-2020

KPMG

## Drivers

- Technology providers are driving the redundancy of their on-premise solutions to accelerate the adoption of cloud-based solutions
- Technology start-ups have developed new "born-in-the-cloud" solutions that are also driving cloud adoption
- There is a drive to reduce IT capital investment and the ongoing operational costs to maintain this infrastructure
- More devices are being connected to the Internet (e.g. washing machines), and organisations need to transform to further take advantage of all this "new" data that is being collected
- Cloud-based tools and applications enable easier and quicker ability to analyse and mine large volumes of unstructured data to enable quicker and more intelligent decision-making, and improving an organisation's ability to monetise their data

**Martin Vipond**
Partner
Digital Consulting

# Data: Cloud Computing & Data Sovereignty

## The infinite value of data in the sky

The ongoing use and maintenance of "on-premise" IT systems and databases is fast becoming a thing of the past. The world is rapidly moving towards cloud-based solutions and data storage. The key difference with cloud solutions is that the organisation rents access to IT software and data storage from a service provider – and this could (in theory!) mean that the organisation's data is stored anywhere in the world.

Major technology providers are focussing on cloud solutions which is driving their own legacy solutions into redundancy. In addition, technology start-ups like Coupa and Workday have accelerated this trend by championing new, flexible "born-in-the-cloud" solutions that sometimes surpass the traditional technology solutions from a cost-benefit perspective.

The decision whether to migrate to the cloud should no longer be a topic of discussion. It is the new normal that organisations will have to adopt sooner or later – the question is when and how?

### Where should we host our data?

Once the decision to migrate to the cloud starts, tougher decisions will present themselves:

#### Which cloud service should we use?

There are many established cloud service providers to choose from, led by the technology powerhouses of Microsoft, Amazon and Google but with challenges from Alibaba and IBM and the like. In choosing a provider, customers weigh up factors such as the technology roadmap of the provider which of their IT systems are cloud-ready, total cost of ownership, mitigating the risk of "lock in" and – critically from a regulatory perspective - where the customer's data will actually be stored.

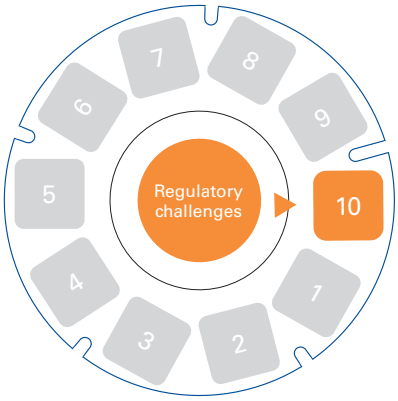
It is the last point leads to the concept of "data sovereignty". This refers to i) Where will our data be stored? and ii) Whose jurisdiction and legal framework would apply?

Most large cloud service providers will have an established network of data centres in a selection of countries. They can thus store data for clients across the globe without this data having to travel too far (i.e. across continents) which could impact IT performance and response times.

However, these cloud data centres typically service a large geographic region, (e.g. sub-Saharan Africa) rather than specific countries. This results in a challenge where a preferred cloud provider does not provide a data centre in your country, leaving customers no choice but to store their data outside of their borders.

A few challenges arise: i) Do the local regulations allow for data to be stored outside the country's borders? And ii) If data is stored outside of their borders, what additional regulations (and complexities) are now applicable?

Regulators have seemed to be prudent in their regulations and guidance, favouring business enablement e.g.




the Prudential Authority's Directive 3/2018 that allows for the use of cloud computing, but requiring a strict governance framework to ensure there are controls to over the storage and use of this data. However, organisations are required to make formal submission to their regulators to secure approval to use cloud computing services.

### Whose rules do we have to comply to?

The next challenge is understanding the regulatory landscape of the foreign jurisdiction(s), but not only that of the hosting country but there needs to be consideration of foreign citizens whose data the organisation may be processing. For example, if an organisation is processing data of a citizen of a European Union member states the EU's General Data Protection Regulations (GDPR) would be applicable.

Multinational organisations face an incrementally complex regulatory landscape. Let's say an organisation has a presence in South Africa and Australia, and they choose to use a cloud datacentre located in Malaysia. There are three jurisdictions that come in to play, which greatly increases the compliance burden (and costs!).

### Why are geo-politics an important factor to consider?

Would the US government allow its organisations store their data in a Russian cloud datacentre? Certainly not. But the US has numerous cloud datacentres located within their boundaries and so US organisations are not faced with any such challenges.

If we consider developing nations, they have very little power or choice as to where their data will be stored. Using a cloud datacentre in a country with whom they there are political tensions may be their only choice. Another point to consider is also where the data is being replicated to as part of the backup and disaster recovery processes. The primary data centre may be a friendly nation, but what if the backup datacentre(s) are located in a hostile territory?

## Key actions

- Define the organisation's exact cloud computing requirements. Considerations should include (amongst others) the extent of cloud usage, the ability of the organisation to migrate to the cloud, geographic landscape of the organisation, IT performance and response times required etc
- Investigate the different cloud service providers' offerings and how their services will address your organisation's cloud computing needs. Understand what primary and secondary datacentre locations exist, what are the regulatory requirements of the relevant foreign jurisdictions
- Define a cloud computing strategy as part of the greater technology strategy. This should cover solutions to address the above requirements and considerations investigated above
- Perform a detailed analysis of all the foreign jurisdiction regulations as they pertain to data storage and usage to define a complete data regulatory landscape. Implement internal processes and structures that will then be able to manage and document compliance to the full regulatory landscape
- Confirm that the chosen cloud datacentre will provide the relevant IT performance and response times that will be acceptable to your organisation such that it does not hamper the user experience or impact time-critical transactions
- Perform a longer term cost estimation of the costs to host in the cloud. Cloud service providers typically charge by the amount of data is being stored in the cloud. As the rate and volume of data collection increases, the costs to host in the cloud could far exceed initial cost estimations in the medium- to long-term

# Contact us


**Auguste Claude-Nguetsop**
**Partner & Head of Market Risk – IBOR National Lead**
**T:** +27 82 719 2842
**E:** auguste.claude-nguetsop@kpmg.co.za

**Thomas Gouws**
**Partner**
**Risk Consulting**
**T:** +27 82 718 8432
**E: :** thomas.gouws@kpmg.co.za

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

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

**Beulah Simpson**
**Senior Manager**
**KPMG Privacy Practice**
**T:** +27 60 602 3066
**E:** beulah.simpson@kpmg.co.za

**Derek Vice**
**Partner**
**Financial Services Audit**
**T:** +27 82 711 2519
**E:** derek.vice@kpmg.co.za

**Rudi Sturm**
**Associate Director**
**FRM Credit and Capital Risk**
**T:** +27 82 719 2704
**E:** rudi.sturm@kpmg.co.za

**Marcelo Vieira**
**Partner**
**Cyber Security**
**T:** +27 82 718 8485
**E:** marcelo.vieira@kpmg.co.za

**Martin Vipond**
**Partner**
**Digital Consulting**
**T:** +27 83 454 1812
**E:** martin.vipond@kpmg.co.za


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

kpmg.com/socialmedia