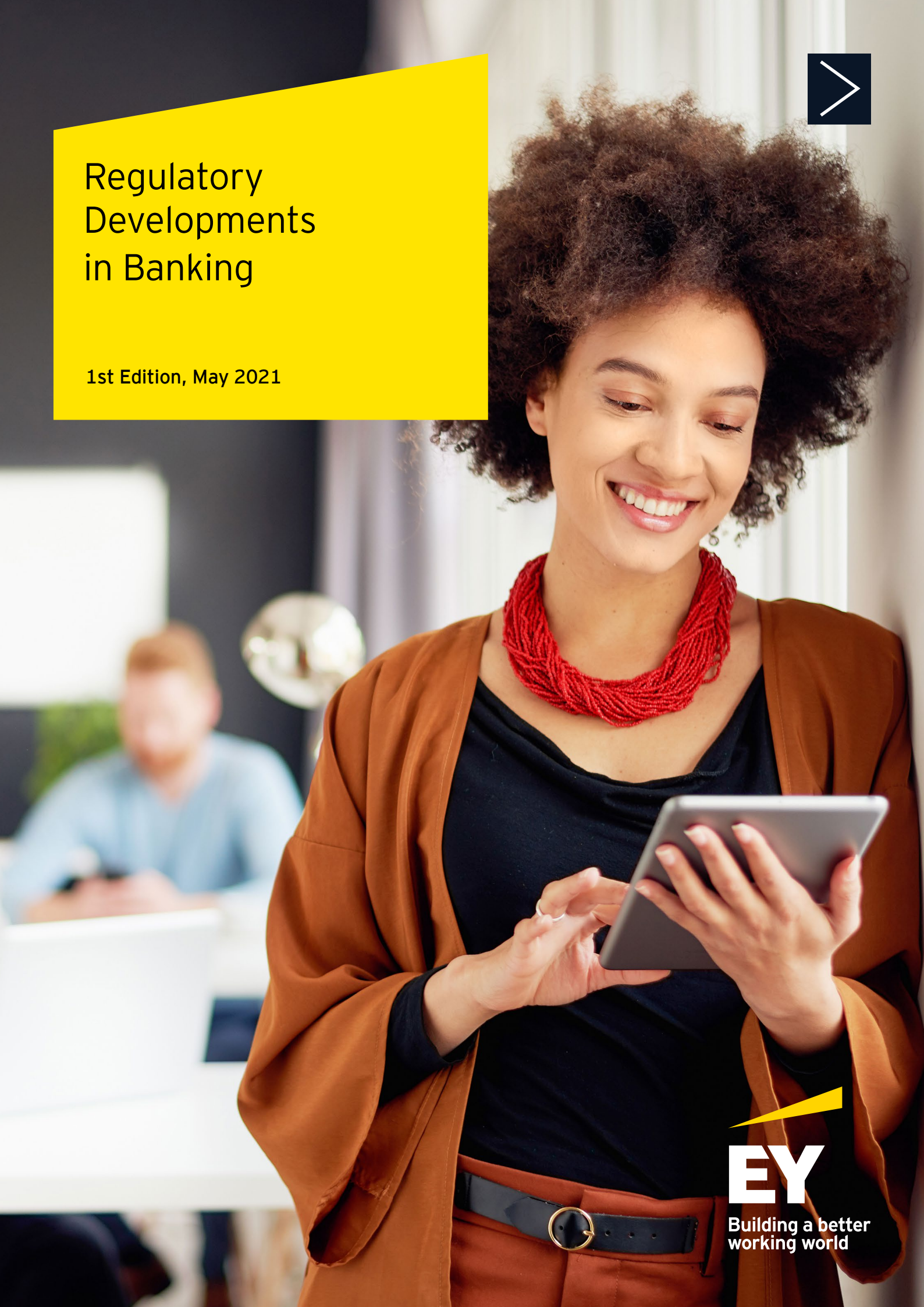
Regulatory Developments in Banking

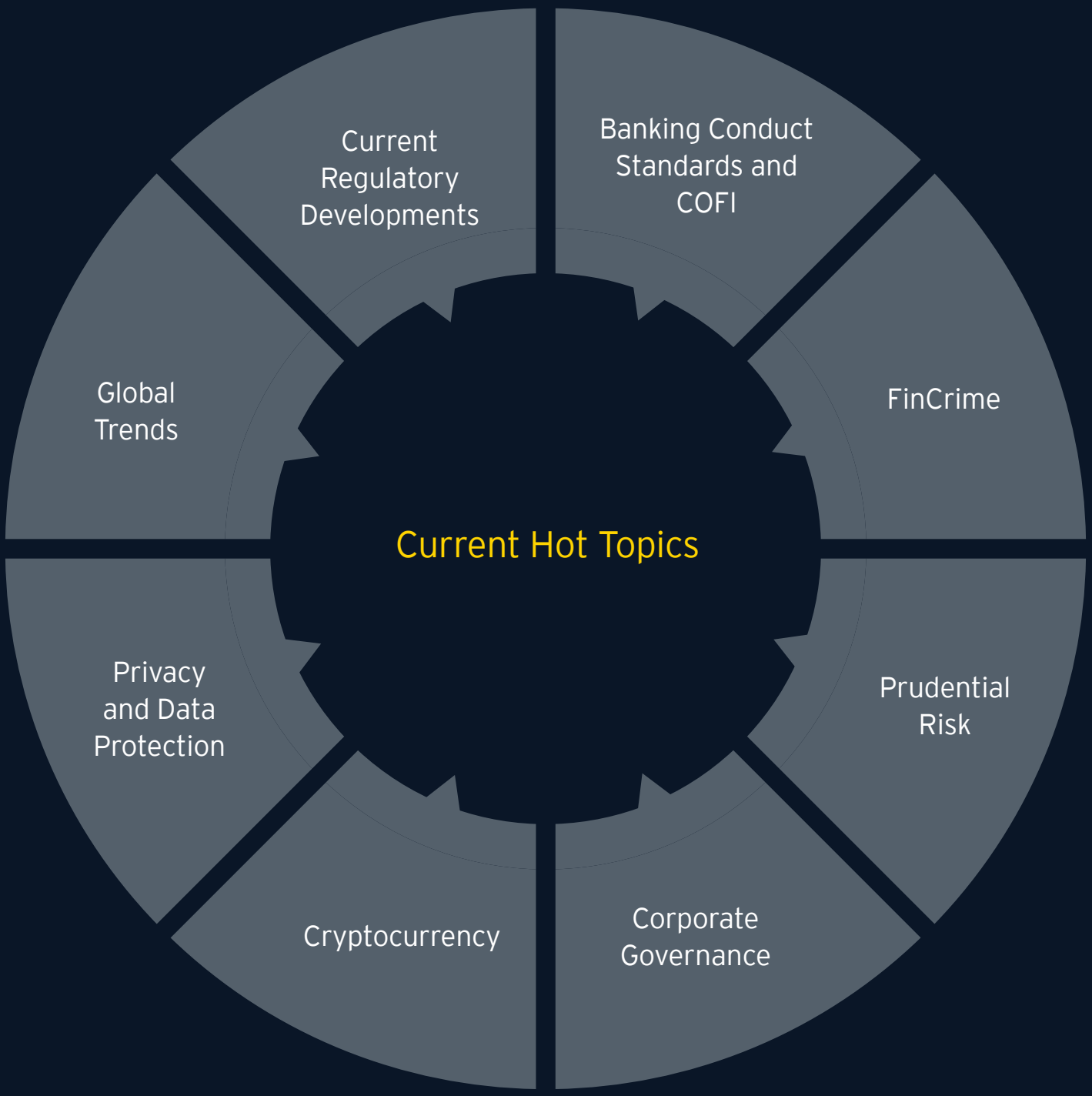
1st Edition, May 2021



EY
Building a better working world

Contents

Please click on below topics to read more



Current Regulatory Developments

Prudential Regulations

Regulatory reform	Proposed implementation date
Standardised Approach to Counterparty Credit Risk (SA-CCR)	Jan 2021
Capital requirements for bank exposures to central counterparties	Jan 2021
Capital requirements for banks' equity investments in funds	Jan 2021
Revisions to the securitisation framework*	Apr 2021
Total Loss Absorbing Capacity (TLAC) Holdings*	Apr 2021
Large exposures framework*	Apr 2021
Interest rate risk in the banking book	Jun 2022
Interest rate risk in the banking book: Disclosure requirements	Jun 2022
Minimum capital requirements for market risk	Jan 2023
Revised standardised approach for credit risk framework	Jan 2023
Revised internal ratings based approach framework	Jan 2023
Revised credit valuation adjustment framework	Jan 2023
Revised operational risk framework	Jan 2023
Leverage ratio – revised exposure definition	Jan 2023
Output floor	Jan 2023 – Jan 2025

** PA has indicated the likelihood that these items only be implemented from July 2021 onwards.*

Conduct Regulations

Regulatory reform	Proposed implementation date
Banking Conduct Standards	Jan 2021
COFI	2022

01

Banking Conduct Standards and COFI

The Banking Conduct Standard requires all banking institutions to comply with the promotion of the fair treatment of customers.

The standard will assist the FSCA to monitor the conduct of banks by ensuring that a Bank's customers are central to the development of products and through the provision of their services. The expectation is that these will be demonstrated through a Bank's customer-centric culture, strategy and governance processes. The compliance deadlines are:

- Sections 1, 2 and 11 effective July 2020
- Sections 3, 4, 5 and 6 to effective March 2021
- Sections 7, 8, 9 and 10 to be effective July 2021

Our detailed Thought Leadership provides an in-depth analysis of the Banking Conduct Standards.

COFI

COFI is intended to streamline the conduct requirements for financial institutions, which are currently found across a number of financial sector laws. This will result in a strong, effective and consistent market conduct legislative framework for all institutions, which undertake financial activities.

The second draft of the COFI Bill was published in December 2018 together with a Response Document that explains the key changes made to the first draft of the Bill, in response to industry comments and engagements held. Some of the key changes made between the first and second drafts of the COFI Bill include the following:

- Application of the COFI Bill in relation to existing legislation
- Approach to licensing
- Focusing transformation to tangible targets
- Approach to medical schemes sector
- Application to the non-retail market

Impact on the credit sector

The National Credit Regulator will continue to regulate credit providers and all credit agreements as defined in the National Credit Act, 2005. COFI will however focus on credit providers who bring the most conduct risk to the largest number of vulnerable customers in the market. Banks will be supervised to ensure that their governance arrangements are sound, their financial services meet customers' needs and that customers are not exposed to undue post sale barriers.

Impact on the National Payment System

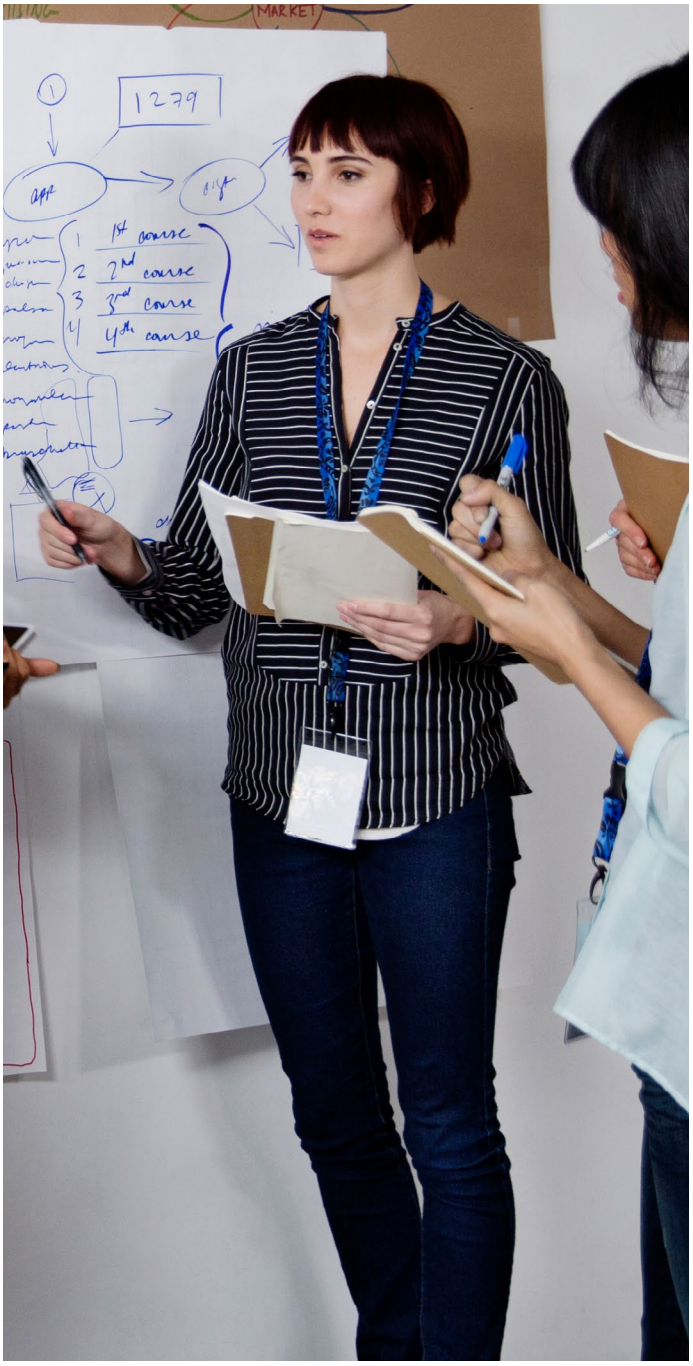
The payment environment has been broadly defined and payment activities will be regulated by FSCA. The Prudential Authority will continue to oversee the payment system from an integrity, stability and efficiency perspective, whilst the mandate of the FSCA will require co-operation with the Prudential Authority to ensure that conduct outcomes are considered across all components of the payment infrastructure.

Impact on the Pension Funds Act

It has been proposed that retirement funds will have to be licensed under both the PFA and the Bill. These funds will be subject to the requirements of both laws to ensure consistency in the manner in which customers are treated. Retirement fund benefit administrators and other service providers, currently regulated under the PFA, will, in future, only be licensed and authorised under COFI. There will be a transitional period to ensure alignment between the provisions of the PFA and COFI

Impact on Collective Investment Schemes Control Act (CISCA)

COFI will regulate investment arrangements that bring together contributions from the public for purposes of investing such contributions in order to generate a return. Accordingly, traditional products such as collective investment schemes ("CIS") and private equity funds will now be licensed under the framework of the bill. The category of pooled investments currently contemplated under CISCA is retained under COFI, whilst provision has been made for another pooled investment product to be known as "alternative investment products". This will ensure that there is sufficient regulatory oversight, considering the risks that different products pose to different customers. The licensing requirements will, in turn, distinguish between the licensing for a pooled investment product contemplated under a CIS and pooled products classified as alternative investments. COFI will replace CISCA in its entirety.



02

FinCrime

Firms are constantly seeking to evolve and adapt in a complex, connected and ever-changing world to reach newer levels of sophistication, where known and unknown risks proliferate.

Financial crime in the financial services sector is one such risk. In fact, it's one of the largest systemic risks to the global economy, with devastating impacts on businesses and communities around the world.

The impact of regulatory investigations and fines over the past 10 years on the financial services industry has been huge, from both a cost and operational perspective. These costs have included the execution of large-scale investigation and remediation projects. Firms not faced with regulatory inquiries have, nevertheless, incurred increased costs through reinforcing their compliance control frameworks to ensure that they stand up to regulatory scrutiny. In South Africa, there is likely to be an increase in fines and penalties imposed by the respective regulators for inadequate Risk Management Compliance Programs (RMCPs) and related controls as soon as inspections resume to normal activity post the Covid-19 pandemic.

The South African financial crime regulator, the Financial Intelligence Centre (FIC), models the country's anti money laundering and counter terrorism financing (AML/CFT) regime on the guidance set out by the Financial Action Task Force (FATF), the international AML standards setting body. As a FATF member country, South Africa is routinely inspected by the FATF and needs to demonstrate adherence to the FATF guidance and recommendations. To this end, the Financial Intelligence Centre Act (FIC Act) imposes various obligations on accountable institutions related to identification and verification of clients, transaction monitoring and reporting and record keeping, among others.

The FIC Act was amended in 2017 to improve the protection of the integrity of South Africa's financial system and strengthen its ability to prevent and punish financial crimes like money laundering, illicit capital flows, tax evasion, corruption, bribery and financing of terrorism. The FIC Amendment Act introduced various new requirements such as:

- Risk-based approach
- Customer Due Diligence (CDD) measures
- Record keeping requirements
- Risk Management and Compliance Programme
- Targeted financial sanctions

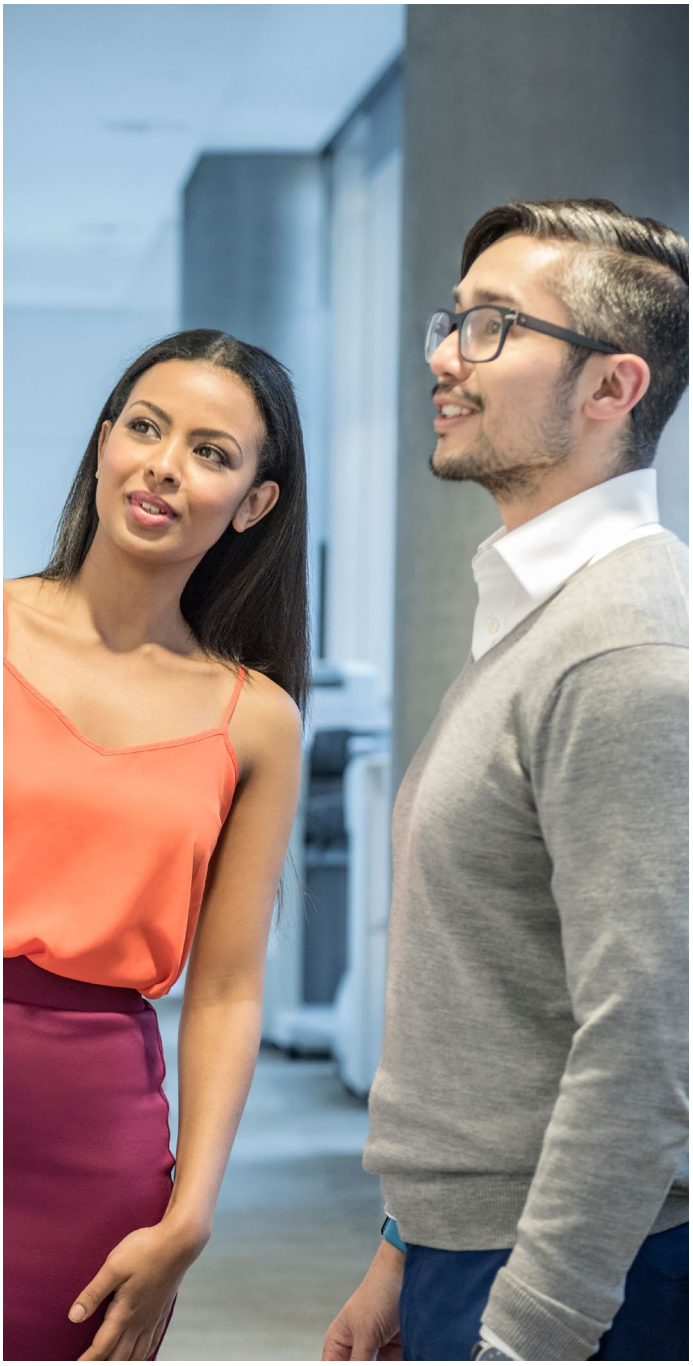
In order to give effect to these new requirements, institutions are required implement enhanced governance and training as well as ensure that they appoint a compliance officer responsible for oversight of FIC Act compliance.

As a result of the new requirements and risk-based approach, financial crime compliance spending has reached unprecedented levels trying to adopt automation, machine learning and AI into their process to increase efficiency and effectiveness. We note, however, that compliance processes are still dominated by high levels of manual, repetitive, data-intensive tasks that are not only inefficient, but are failing to disrupt fraud and financial crime. Furthermore, at the same time, new technologies, including cryptocurrencies, blockchain and open banking create new risks.

Firms also have an obligation to comply with local data privacy legislation and/or regulations (e.g. the General Data Protection Regulation ("GDPR") and the Protection of Personal Information Act ("POPIA") as part of the money laundering and terrorist financing risk management system. South African financial institutions will need to play a balancing act to ensure satisfactory compliance with the relevant legislation while also keeping an eye on their bottom line.

Currently, cross border transactions are a focus of the Prudential Authority as well as the Financial Intelligence Centre. The regulators recently published a draft joint communication paper which sets out the requirements for instances when institutions process electronic fund transfer (EFT) transactions, both domestically and cross-border.

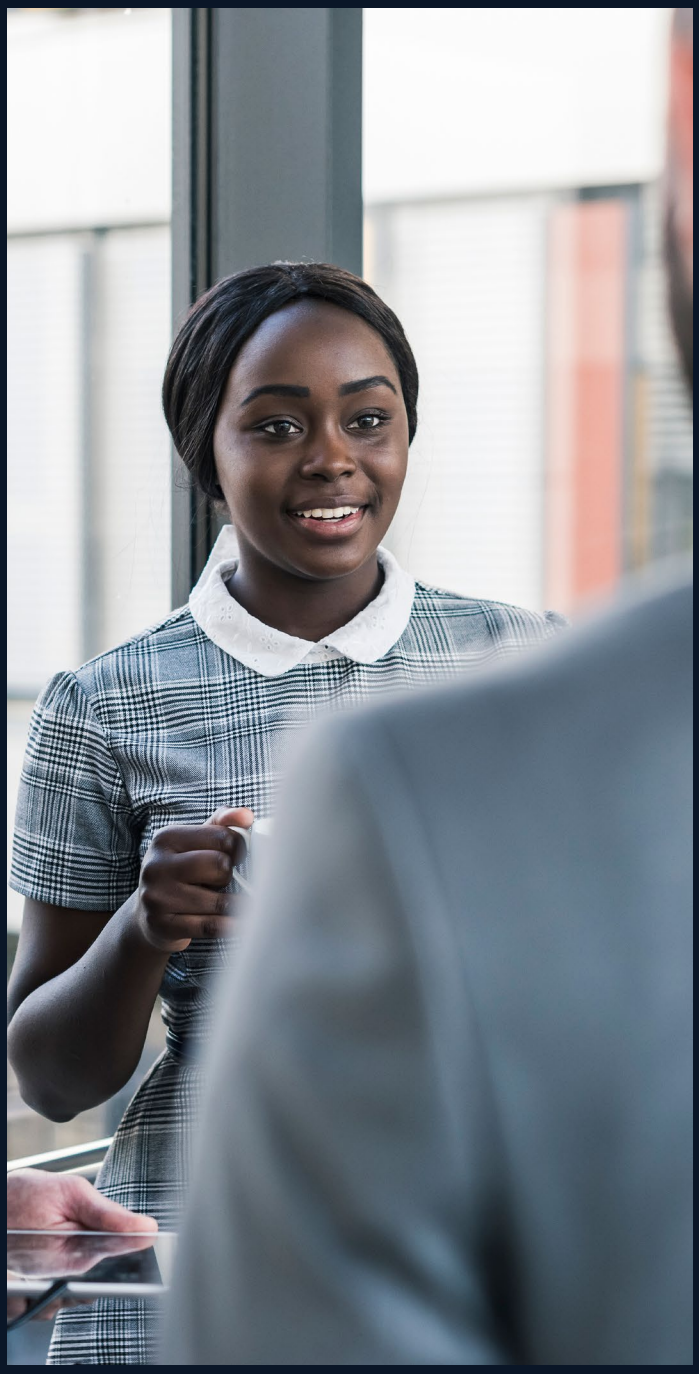
The draft paper indicates in what circumstances institutions needs to report cross-border transactions, what minimum information needs to be requested before undertaking or accepting an EFT, what information should be included as part of the transaction and the circumstances for refusing or suspending a transaction. The document was published for consultation purposes an comments were received from the relevant industries. The paper is currently in the process of being finalised by the Prudential Authority and a final version is expected shortly.



03

Prudential Risk

The Prudential Authority's flavour of the year topic for 2021, the impact of new technology on Banks, highlights the importance that technology plays in the local and global banking arena.



As organisations embrace the new digital era and further build on their existing digital capabilities or adopt new technology, so too will the regulatory oversight to ensure the sustainability and operational resilience of the banking system. It could be argued that the Impact of new technology on Banks is a "build-on" to the previously issued directives relating to Cloud Computing and Data Offshoring, together with the focus placed on Cybersecurity and IT risk by the Prudential Authority. As systemically significant organisations have already adopted and conformed to the prior Directive/Guidance Note, the focus of these organisations is operational resilience.

Recovery and Resolution Planning, albeit well established and embedded amongst key market players, will continue to be a focus of the Prudential Authority in an effort to ensure operational sustainability of the financial system.

In light of the IFRS9 Covid-19 relief in respect of impairment classification, many banks have noted a significant shift in their credit impairments given the higher level of credit restructures. The impact on their respective credit portfolio will be noted in their current financial reporting and it is expected that further guidance will be provided by the Prudential Authority on assessment of the sustainability of the higher risk levels to the financial system.

Per the Regulators Regulatory Strategy roadmap, regulations related to the supervision of financial conglomerates is expected to be promulgated to obtain a holistic view of group-wide activities, intragroup transactions and large exposures which, among other things, may not be captured under Level 2 supervision (consolidated supervision). These requirements are expected to be approved by parliament in 2021 and come into effect on 1 January 2022.

04

Corporate Governance

In October 2018, the Prudential Authority issued the Banks Act Directive 4/2018 pertaining to matters related to the promotion of sound corporate governance, and in particular to the appointment of directors and executive officers for locally controlled Banks. The compliance deadline is January 2022.

The Prudential Authority's supervisory review and evaluation process is expected to proceed throughout 2021 and will assess a bank's governance policies, processes and practices which would consider the bank's risk profile and systemic importance.

05

Cryptocurrency

Discussions over the past years around the introduction of regulating crypto currencies continue to progress well and have resulted in the FSCA considering measure to regulate the market thereby offering a level of protection to consumers. The FSCA says it is working with the Intergovernmental Fintech Working Group (IFWG) to better understand and regulate "where appropriate", crypto assets in SA and advises retirement fund trustees to remain vigilant in their fiduciary duties before allowing investment managers to expose their fund assets to cryptos.

The FSCA has published a draft declaration that proposes to declare crypto assets as financial product in terms of the FAIS Act.

The position paper[1] outlines the following as reasons for the "need to develop a regulatory and policy response to crypto asset activities in South Africa"

- Crypto assets are a form of fintech innovation that may impact on the financial sector of the country,
- Crypto assets operate within a regulatory void as no globally harmonised approach or position has been reached as yet,
- Crypto assets may create conditions for regulatory arbitrage while posing risks, and
- Crypto assets may become systemic, as interest, investment and participation in crypto assets continually grows.

The regulation of Crypto Assets when it lands will be facilitated by the National Payment System Department of the Prudential Authority.

1 **[20200414 IFWG Position Paper on Crypto Assets.pdf (treasury.gov.za)]**

06

Privacy and Data Protection

Organizations have been granted a grace period of one year to normalize and implement the requirements of the law within their risk and compliance frameworks and must be able to demonstrate compliance by 1 July 2021.

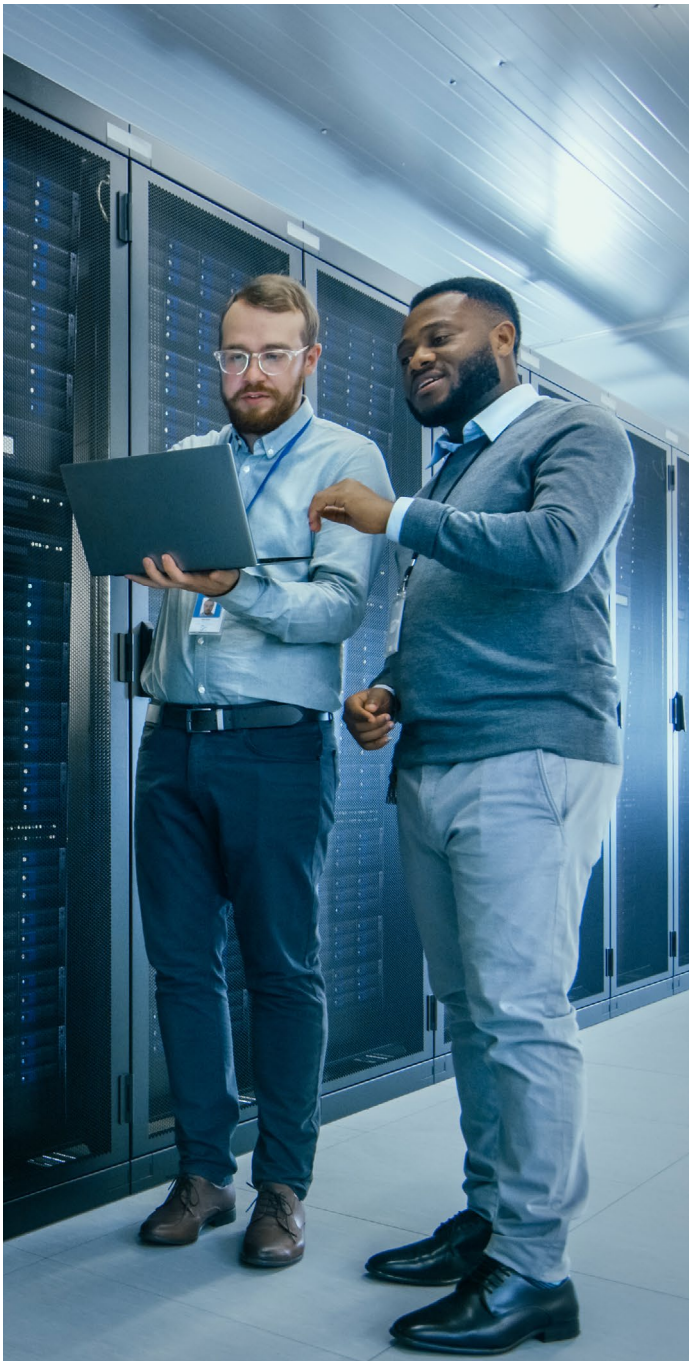
Having recognized the need to regulate the use of personal information within South Africa, the Protection of Personal Information Act (POPIA) was enacted, with the bulk of sections commencing on 1 July 2020, effectively ushering South Africa based organisation into the new era of data privacy.

What are the next steps?

1. Register your Information Officer and Deputy Information Officer(s) with the Information Regulator. As per a media statement issued by the Information Regulator on 24 March 2021, the registration of Information Officers and Deputy Information Officers will commence on 1 May 2021. The registration process will be an online one as per the statement.
2. Establish a robust privacy framework to demonstrate compliance to the requirements of POPIA. Organizations will need to ensure that the framework meets the expectations of the Information Regulator. This will imply answering the following key questions:

- The Deputy Information Officer must report to the highest management office within an organization. Who should be appointed as the Deputy Information Officer and where should this function sit to meet this requirement?
- Are the duties and responsibilities of your Deputy Information Officer in conflict with other duties assigned to him or her?
- Are you considering data protection issues as part of the design and implementation of systems, services, products and business practices?
- Do you have privacy notices/statements at each point of collection of personal information?
- Do you have a functional process to identify, assess and address data privacy risks in line with the requirements of POPIA? How integrated is this process with your overall Enterprise Risk Management (ERM) framework?
- Do you have a clear picture of what types of information you hold, for what reasons they are processed and where they are stored?
- Have you developed and communicated a set of policies and procedures to support the privacy framework?
- Do you know within how many days you are required to respond to a data subject request? Have you assessed whether your organisation is prepared to respect this timeframe?
- Would your employees recognise a personal information breach when they saw one? Would they ignore it? Would they know what to do about it?
- Do you have appropriate skills and resources to support the privacy framework?
- Do you have sufficient overview of the privacy posture of your departments and service lines?
- Are you disposing of personal information when the retention period has lapsed? Have maximum retention periods been defined and personal information tagged for disposal accordingly?
- Do you know whether your service providers are processing your data as per your expectation?

- Are you sure that you are processing your clients' and employees' data as per their expectation?
- Are you ready to demonstrate proof of compliance to the Information Regulator as from 1 July 2021?



https://www.ey.com/en_za/cybersecurity

https://assets.ey.com/content/dam/ey-sites/ey-com/en_za/generic/ey-popia-report-2020.pdf

07

Global Trends

Technology and Data

The acceleration of the digital agenda due to the pandemic will require a timely response from regulators. We are now seeing more coherent digital strategies being developed that will aim to pick up all the key elements.

As financial institutions take advantage of the current leap in digital engagement and continue to develop transaction execution and service offering capabilities on the back of the momentum gained during the lockdown, including a significant switch to a non-cash environment, we can expect to see the emergence of a coordinated policy framework for the new digital era of financial services.

In this context, fair treatment of customers and data privacy and protection must be among key policy considerations that accompany the digital acceleration, rather than an afterthought. We can expect to see requirements for greater transparency around how data analytics are used, to determine creditworthiness for example, in order to identify and prevent built-in bias that leads to undesirable outcomes via negative screening, filtering and discrimination.

> Local and International Supervisors will continue to develop clear markers that regulatory frameworks must be constructed, or adapted, before Big Tech's new wave of payment systems, mobile services, data owners, digital currencies and other FinTech applications generate systemic issues, both domestically and internationally

ESG

Sustainability will return to centre stage in 2021. An immediate boost is the new Biden administration's decision to re-engage in global climate talks, with both Washington and Brussels talking about linking trade and climate agendas. This is accompanied by renewed worldwide regulatory pressure for adoption of sustainable finance frameworks and growing support for the agenda from large international banks, investors and corporates. The foundation of climate risk regulation must now be put in place via a taxonomy that can serve as a list of "green" economic activities and a basis for a series of disclosure requirements for corporates, financial market participants and financial products.

Regional and national efforts are underway, and we expect to see further momentum throughout the year. For example, Singapore and Hong Kong have been driving disclosure and taxonomy initiatives in Asia-Pacific, the Monetary Authority of Singapore (MAS) is developing standards for insurance, banking and asset management sectors, and the Hong Kong Securities and Futures Commission (HKSFC) has issued proposals for climate risk disclosure by fund managers and with other regulators and is starting on a sector-wide taxonomy to be aligned with the EU and Chinese efforts.

Prudential risk

Regulators will be focused on supervisory stress testing and banks' own internal stress testing in late 2020 and 2021 as a means of testing the asset quality of banks and understanding capital vulnerabilities. It is not evident that regulators are changing their stress test methodologies significantly, but Covid-19 exposures and the environmental, social and governance (ESG) agenda are creating new data and stress testing demands. Banks' own methods will need to expand to match their evolving credit review processes that include deeper sectoral and supply-chain analysis and a focus on borrowers that are more highly leveraged.

The Group of Central Bank Governors and Heads of Supervision (GHOS), the oversight body of the Basel Committee, has signaled an end to the post-2008 financial crisis policy agenda. The revised timeline for Basel III implementation has been in place since March 2020, and the GHOS has stated that any further potential adjustments to Basel III will be limited in nature and consistent with ongoing evaluation work. In terms of regional implementation, pandemic recovery measures will take priority ahead of assessments of the remaining elements of Basel III and IV.

08

How can EY Help

EY has a dedicated Financial Services Consulting practice, which includes Risk Management, Technology, Process and People. This gives us deep industry knowledge in all aspects of the financial services industry, allowing us to tailor integrated solutions to our clients' specific needs.

Our Financial Services Risk Management (FSRM) practice, which forms part of the Financial Services Risk domain in Business Consulting, is experienced within financial services firms and regulators in various jurisdictions and composes of a variety of skills across the insurance and banking sectors. We combine local regulatory and legislative knowledge with best practices in global prudential regulation as well as governance,risk and compliance (GRC).

Through our fully integrated global Prudential, GRC and Actuarial networks, we ensure that we are at the forefront of global regulatory developments. We leverage this to approach compliance and risk management not only from a regulatory perspective, but also from a strategic perspective.

Market Conduct:

The FSRM team can assist in helping financial services organisations design their interactions with customers and counterparties, to deliver fair outcomes and market integrity, and effectively manage associated regulatory, reputational and strategic risks. We can do this by:

- Assisting our clients with the design and development of market conduct frameworks, organisational culture frameworks and assist in implementation thereof, and
- Performing gap analyses against the regulatory requirements and benchmarking compared to local and global practice of existing market conduct frameworks.

Governance, Enterprise Risk and Compliance:

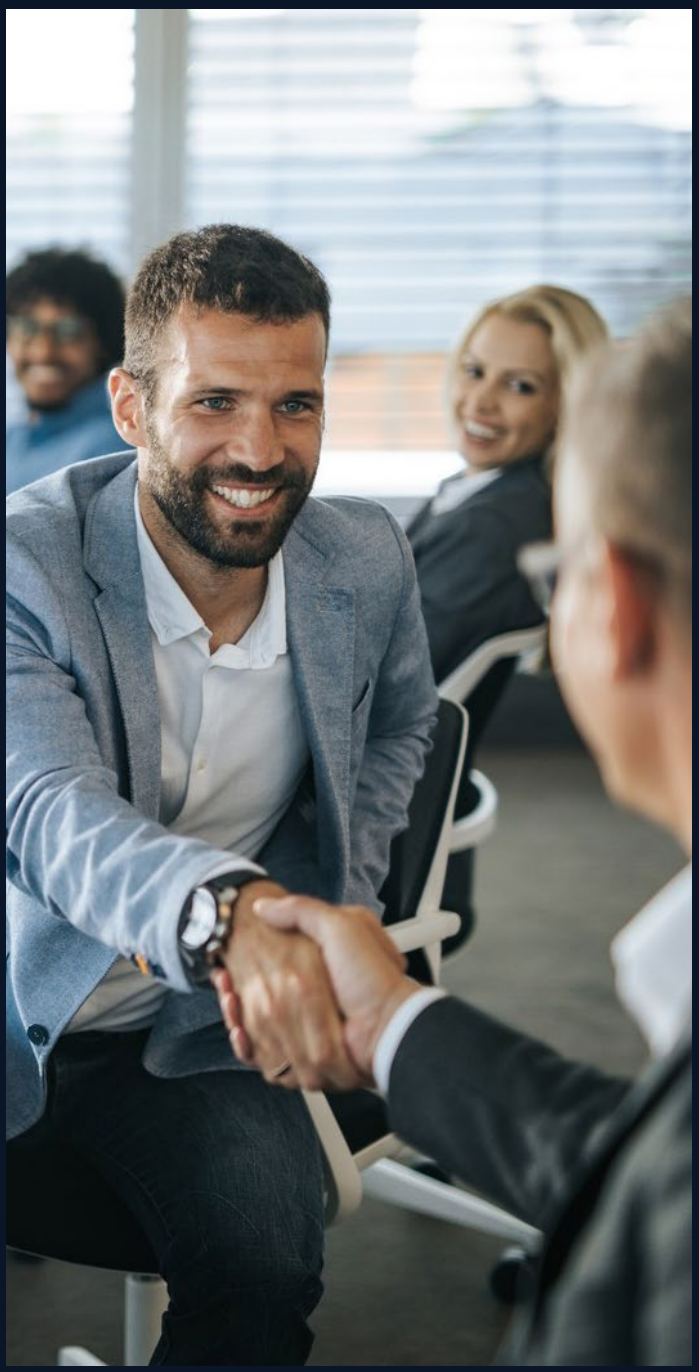
Within the GRC space, our FSRM team can assist in:

- Reviewing Governance Policy and Control Adequacy,
- Assessing the maturity of Risk / ERM and Compliance Functions (including benchmarking to best practice),
- Developing or assessing 3rd Party Risk and Binder Risk Management Frameworks,
- Designing, implementing or enhancing Credit Risk Frameworks,
- Establishing ESG governance frameworks and design disclosure,
- Developing, implementing or enhancing Model Risk Management,
- Setting up or reviewing Recovery and Resolution Planning,
- Assisting in preparing for the requirements under the Financial Conglomerate Supervision/Regulation,
- Assisting in selecting GRC solutions and implementing these, and
- Establishing and management of Regulatory Inventories and risk controls.

Prudential Risk:

The services offered to banks and insurers include:

- Reviewing Regulatory Capital Requirements (BA Returns and Quantitative Returns),
- Reviewing or performing ICAAP/ORSA,
- Assisting in Capital and Balance Sheet Optimisation/ Management,
    - Developing Economic Capital models,
    - Performing reviews of Pillar 3 Requirements for Banks,
    - Supporting in IBOR/JIBAR transition implications and preparation,
    - Optimisation of overall financial resources
- EY can assist with defining the prudential regulatory framework and the pro-active strategic response to mitigate the implications of these regulations on key financial indicators.
- EY's global regulatory network leverages regulatory knowledge on an international scale. We can support our clients in understanding and addressing the most critical financial and compliance impacts for their business as a result of regulatory change and help them to implement solutions on a cross-border basis to support compliance wherever they operate.
- In today's environment of heightened and evolving regulation and structural changes, our professionals can work side by side with our clients to interpret new rules as they are issued. Through this collaboration, any compliance and operational changes that are required can be identified quickly and processes can be established to implement them efficiently.



Contacts

Marius Van Den Berg
Partner, EY Consulting
Banking and Capital Markets Leader
marius.vandenberg@za.ey.com

Neil Maree
Partner, EY Consulting
Prudential Risk
Neil.Maree@za.ey.com

Threshern Naidoo
Senior Manager, EY Consulting
Financial Services Risk
Threshern.Naidoo@za.ey.com

Shameem Goolamun
Associate Director, EY Consulting
Africa Data Protection and Privacy Leader
+230 5774 9072
shameem.goolamun@mu.ey.com

Manuel Caldeira
Associate Partner, EY Assurance Services
Forensic & Integrity Services
manuel.caldeira@za.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

ED None

ey.com