



Securing the  
future of banks  
from risk and  
regulatory  
uncertainties

The evolving landscape  
and the way ahead



**T**he capital market industry is facing critical business challenges because of the continuously evolving and diversifying regulatory environment. Ongoing regulatory requirements, diversified product offerings, enhanced customer expectations, and fierce competition has become the new normal for banks today. Growing stakeholder and investor expectations in these volatile economic conditions are adding to the pressure on banks. Meeting the regulatory deadlines while striving for cost efficiencies is the biggest challenge for the banking sector.

While many regulatory change initiatives have their roots in the global financial crisis, which occurred a decade ago, there are other recent contributing factors such as cyber threats, data attacks, the rise of digital money, and unpredictable political scenarios. Cyber threats have increased and kept pace with the technological advancements and innovative growth within the industry. There have been multiple data breach cases recently, which have increased the focus of regulators and bankers on data protection and cybersecurity. Emerging technologies such as the Internet of Things (IoT), Distributed Ledger Technology (DLT), and Artificial Intelligence (AI) have the capability of revolutionizing the market channels and its intermediaries. However, everything comes at the cost of security and legal risks.

The capital market is likely to face a number of strategic and regulatory challenges in the coming years. Let us look at the key interrelated risk and regulatory themes that will demand the attention of the capital market industry.

### Political uncertainty

Brexit may bring in the end of ‘passporting’ for services and transactions for banks. This will potentially force them to scale up their operations separately in the UK and the EU and reevaluate their wealth management products and transaction booking models.

Regulatory divergence in the UK and EU will further increase banking overheads. In the US,

elimination of the Volcker Rule might lead to banks indulging in risky trading, thus compromising the interest of the investors. Besides, the NAFTA retooling will have an immense impact on the trade arrangements among Mexico, Canada and the US.

### Multiple regulatory deadlines

The year 2018 is marked with multiple regulatory deadlines in the European markets like the General Data Protection Regulation (GDPR), MiFID II, Prospectus Regulation and the Payment Services Directive II. Banks will also have to deal with new accounting rules like IFRS 9, focusing more on asset quality and non-performing loans, and the collective impact of these issues on stress tests and resolution plans. In order to meet the regulatory targets, banks are struggling hard to put together implementation plans and align their resources primarily to fulfil the regulatory requirements affecting their service delivery. This has resulted in constant tightening of regulatory capital adequacy, coupled with cost pressure.



**Meeting the regulatory deadlines while striving for cost efficiencies is the biggest challenge for the banking sector.**

### Cyber security, data protection and privacy

The massive ransomware attack in the first half of 2017 made cybersecurity the biggest concern of the financial market. With the banking sector progressing towards digitalization, cyberattacks are also increasing in both number and intensity. Cyber criminals are using the power of cloud services, mobile technologies, AI and Machine Learning (ML) to set up cloud bots to take over processing control, launch Distributed Denial of Service (DDoS) attacks via cloud, and hack various

authentication and verification technologies. This is fostering security threats and fear among both banks and the banking customers. Therefore, regulators are now focusing more on data protection. In the EU, the implementation of the GDPR will lead to a greater degree of data protection harmonization across nations. Besides, the US has introduced DFS regulation in March 2017, which enforces banking institutions to follow and implement risk and security governance programs, design incident management plans, produce compliance reports, appoint a Chief Information Security Officer, and conduct regular risk assessments.

### Rise of fintechs


The banking sector is under tremendous pressure from regulatory bodies to improve their capital positions. This is forcing banks to adopt revolutionary changes such as digitalization and innovation to realize cost reductions and maintain profit growth. As a result, banks are increasingly partnering with IT driven financial start-ups called FinTechs to transform their legacy systems. These firms are assisting banks in creating deeper retail customer connections and meeting demands of the tech-savvy retail customer base. However, the unconstrained attribute has led to risks related to the privacy and security of customer data. Since FinTechs exist on technology, it also opens the gate for cyber fraudsters to attack and exploit sensitive customer data. Besides, money laundering and capital control risks are also involved. Regulators are working on designing regulations for FinTechs against this high-risk market.

### Innovation and digitalization

DLT such as Blockchain, which underpins the Bitcoin cryptocurrency, is the current headline-grabbing technology in the financial market. While the potential of this technology is game changing, there is a risk of end-point security attack. Therefore, a lot of legal, regulatory and security risk questions are being raised on the adoption of Blockchain. Although as of now, there is no clarity, we will soon have guidelines on regulating cryptocurrencies and the Blockchain technology.

## How should banks address these challenges?

In order to stay relevant in this ever-changing financial climate, banks need to find ways to overcome the risk and regulatory challenges as well as the resulting operational and IT change management challenges. They must be well prepared and resourceful to capitalize on the potential benefits of the changing times. With the pressure of meeting regulatory deadlines in the EU, banks should put a control on their strategic spend, and invest on digital transformation by implementing innovative digital technologies such as Robotic Process Automation (RPA), ML, Artificial Intelligence, analytics etc. to meet the regulatory demands of the EU region. Banks can automate their compliance and regulatory reports by using RPA to reduce the resourcing burden. Besides, analytics and AI will enable them with complete data flow picture, thus assisting in meeting the required regulatory demands. This can aid banks in doing a complete study of their information flow, thereby, setting up a robust Data Loss Prevention (DLP) solution plan to mitigate data loss and security risks.



**Banks should put a control on their strategic spend, and invest on digital transformation by implementing innovative digital technologies.**

Banks must prepare themselves to defend against potential attacks and enable advance security warnings. They should set up network services that are robust enough to signal the potential threats and risks, and design infrastructures, which can immediately respond to these attacks by locking down security systems.

Technology alone cannot save banks from cyberattacks. A strong governance model should be established wherein; the information security,

risk assessment, and periodic audits are considered integral parts of the operating model.

Banks need to collaborate with experts who have deep domain knowledge and expertise in designing and implementing contingency plans to mitigate security and regulatory risks. This will empower banks with a holistic approach to prepare for the future risk and regulatory uncertainties. They should focus on optimum utilization of resources, strategic versus tactical

spends, technical solutions to meet regulatory demands, cyber resilience platforms to protect from cyber threats, and a strong governance model for successful implementation.

A future of regulatory uncertainty calls for action and mandates taking decisive steps towards a workable way to drive effective risk management and regulatory compliance.

## About the author

**Nitin Kohli**  
**Head - Enterprise Transformation Practice for Capital Markets, Wipro Limited**

Nitin has over 13 years of experience and leads transformation projects related to business process management, robotics, and digital for

global capital market companies. His expertise areas include investment banking, asset and wealth management, and change management. (With inputs from **Avisha Manjar, Enterprise Transformation Practice for Capital Markets, Wipro**)

**Wipro Limited**

Doddakannelli, Sarjapur Road,  
Bangalore-560 035,  
India

Tel: +91 (80) 2844 0011

Fax: +91 (80) 2844 0256

**wipro.com**

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have a dedicated workforce of over 160,000, serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,  
please write to us at  
**info@wipro.com**

