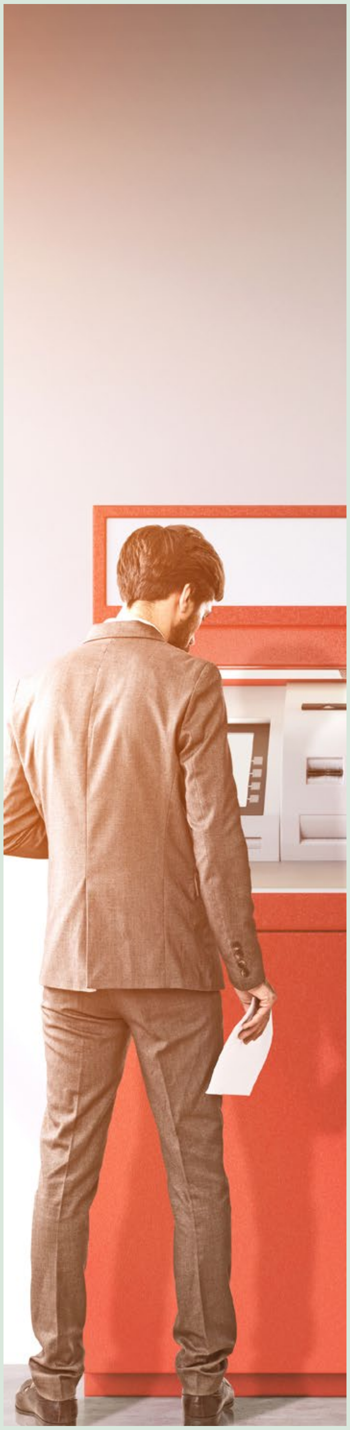
WHITE PAPER



DIGITAL TRANSFORMATION OF ANTI-FINANCIAL CRIME AND COMPLIANCE

Abstract

Financial institutions today use advanced digital tools to become more efficient, profitable, agile, and ultimately better at serving customers who are the mainstay of the banking and finance sector. Despite being a back-end function, anti-financial crime (AFC) and compliance processes have been slow to adopt digital transformation. Considering their complexities, the amount of regulatory supervision, and the fact that most compliance processes are still largely manual, the time is right for automation and digitalization. This paper examines the current challenges in adopting digital transformation in anti-financial crime and compliance processes. It also elaborates on how the latest technologies can help banks transform these critical functions through end-to-end digitalization.

Infosys®
Navigate your next

Introduction

Digital transformation has greatly influenced financial services and banking during the past five years and will continue to do so in the foreseeable future. Customer-driven functions such as lending, payments, commercial banking, and mortgages have all witnessed a digital transformation whereby traditional products, processes, and tools are being upgraded to the latest technologies.

Banks are embracing digital transformation by adopting cloud, artificial intelligence/machine learning (AI/ML), robotic process automation (RPA), Internet of Things (IoT), and connected devices. As the Covid-19 pandemic disrupted banking and industrial operations worldwide, it also brought home the importance of controls to protect against rising incidents of financial crime and improve compliance structures. Digital is one of the most promising ways to achieve such control and security.

Current Challenges in Digital Transformation

Being a vast, complex, dynamic, and all-encompassing space, financial compliance has multiple challenges. Its processes are complex and the associated risks are multi-dimensional. There are multiple regulatory authorities and enforcement agencies to report to for any changes in processes or practices. Moreover, the ambit of regulatory governance has become convoluted with newer entrants such as digital currencies, climate risks and FinTech interventions.

Research reveals that some of the potential challenges are not only limited to these issues but also manifest externally and internally to deter banks from a digitalization agenda. This is further explained below:

Compliance concerns due to increased enforcement – Over the last decade, the number and severity of enforcement actions have increased remarkably. These include a steep rise in fines and penalties as well as the expanding reach of regulatory authorities and agencies. Over the past few months, the current US Securities and Exchange Commission (SEC) chairman issued statements and directives to bring more products, applications, transactions, and assets under surveillance. Apart from anti-money laundering, Basel III, Foreign Account Tax Compliance Act (FATCA), Dodd-Frank, know your customer (KYC), enhanced due diligence, and terrorist financing regulations, the industry is also witnessing a range of newer regulations. These are focused on anti-money laundering, capital adequacy, risk and liquidity management, and consumer protection. The evolving regulatory environment is proving to be a major deterrent for digital transformation.

Resource capacity or technical capabilities – The IT applications used for compliance and financial crime management were not initially designed to be integrated with digital technologies. This has caused serious capacity issues in terms of resources, skills, and technical capabilities. Despite being repetitive, most processes are manual and need human intervention when enforcing and detecting anomalies. The legacy hurdle has been hard to overcome. On-premises compliance systems with mandated manual tasks and limited automation are difficult to integrate with other systems.

Coordination between compliance functions – Different compliance functions and roles have specific accountability and are managed within their specific areas. In future, these functions must leverage a common and cohesive language in terms of technology, processes, control, and risks if they are to adapt to the changing times.

Scalability and efficiency issues – Banks often hesitate from adopting new technologies for fear of increased workload and surveillance requirements. Ironically, the adoption of digital tools and technologies is proven to increase scalability and efficiency, and reduce costs, thereby acting as a panacea for these problems. Nevertheless, the fear of change and upheaval is a serious deterrent. This resistance makes it difficult for banks to derive the benefits of technological advancements in financial crime management, compliance, and regulatory reporting.

Prohibitive costs and return on investment (ROI) concerns – There are several tools and technologies that support robust digital transformation in anti-financial crime and compliance functions. Some of these are cloud migration, AI/ML, IoT, RPA, data analytics, and optical character recognition. These technologies, whether used as-is or in combination with others, require substantial investments in capital and resources. Monitoring and applying digital technologies can be time-consuming as banks must constantly interpret new regulations, create new processes that conform to new rules, meet compliance requirements, and respond to regulators.

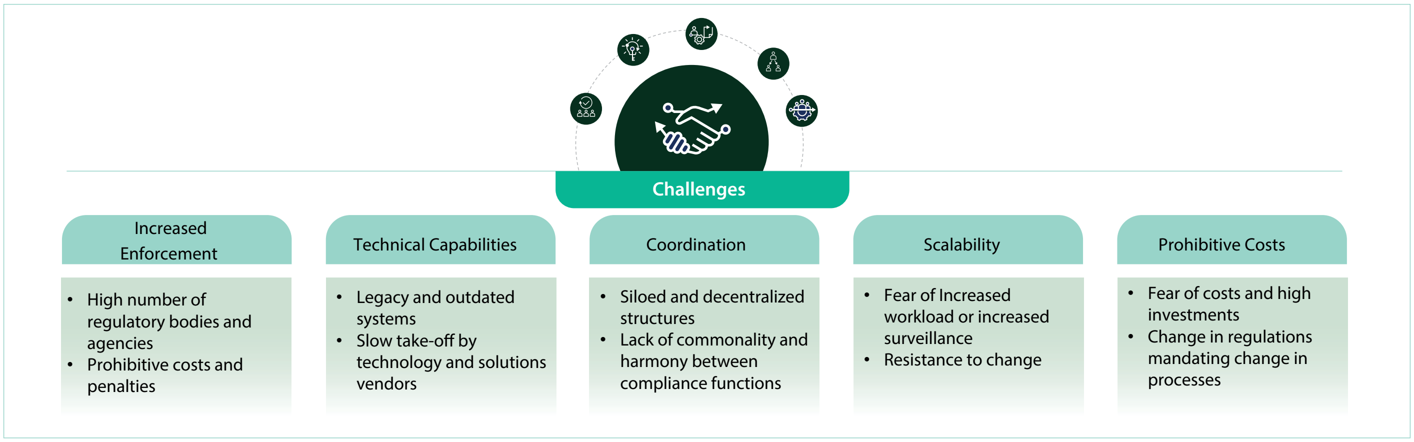

Challenges
Increased Enforcement
High number of regulatory bodies and agencies
Prohibitive costs and penalties
Technical Capabilities
Legacy and outdated systems
Slow take-off by technology and solutions vendors
Coordination
Siloed and decentralized structures
Lack of commonality and harmony between compliance functions
Scalability
Fear of Increased workload or increased surveillance
Resistance to change
Prohibitive Costs
Fear of costs and high investments
Change in regulations mandating change in processes

Figure 1 – Current challenges in digital transformation

Planning for Digitalization of Anti-Financial Crime and Compliance

When the new SEC chairman Gary Gensler took office, he said: "When we fail to root out wrongdoing, or to adapt to new technologies, or to really understand novel financial instruments, things can go very wrong."[1]

It is clear that action is needed across the broad spectrum of activities, processes, tools, applications, and products that constitute anti-financial crime (AFC) and compliance functions. Banks must convert these into digital avatars wherever relevant and possible. Technology and compliance go hand-in-hand. In fact, over the past few years, regulators have been trying to catch up with the implementation of technological advancements in the banking industry by creating new standards for protecting data, regulating blockchain transactions, enabling open banking, and more. Now, it is time to reverse the trend and allow technology to disrupt compliance functions by enabling rapid development and technical innovations in the strategies, products, and applications used for regulatory technology. While the vision seems promising, the actual adoption numbers are, however, alarming.

A 2021 McKinsey survey on digital and analytical transformation revealed that more than 75% of the respondents had not assessed their risk management and compliance areas for avenues of digital transformation[2]. Fortunately, there has been a slow, but steady paradigm shift – new digital propositions in this space have come up either post-pandemic or due to changes in the regulatory structures of different countries. In many cases, the shift is driven by witnessing the benefits of digital transformation in other business areas.

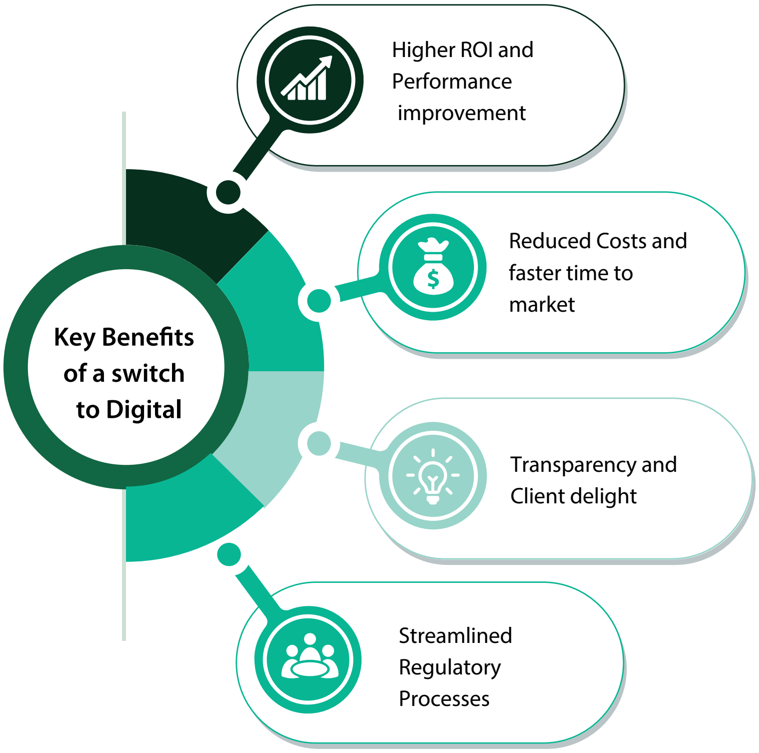

Key Benefits of a switch to Digital
Higher ROI and Performance improvement
Reduced Costs and faster time to market
Transparency and Client delight
Streamlined Regulatory Processes

Figure 2 – Key benefits of digital transformation

Emergence of Digital Technologies in AFC and Compliance

The focus of any anti-financial crime and compliance program is to increase effectiveness, effectively engage regulatory stakeholders, and enhance customer experience and transparency. Digitalizing the value chain enables banks and financial institutions to meet these tenets while enjoying a host of other business benefits. As McKinsey observes, "A well-executed, end-to-end risk-function transformation greatly improves the customer experience, transparency, and accountability, and can also decrease costs by up to 20%."[3]

Banks and financial institutions must prioritize the digital transformation of their AFC and compliance functions, products, and processes to keep up with tech-savvy customers, demanding regulators, FinTech challengers, and stiff competition.

Here is how digital technology can help:

Cloud – The most impactful and powerful among digital technologies, cloud is proven to increase efficiency, reduce cost, and pave the way for adoption of more digital tools. In nearly all cases, cloud is the first step to digital transformation. In line with this, migrating the existing on-premises anti-money laundering solutions, customer onboarding and KYC systems, and fraud and surveillance systems to an application programming interface (API)-based cloud should be the primary step for banks. Enabling 'compliance-as-a-service' would be the ideal way for banking to de-risk their cloud migration journeys. Using automation tools such as DevOps to install and configure compliance solutions on the cloud can speed up the process, resulting in reduced costs and faster time to market.

RPA – Compliance functions involve data-intensive and repetitive manual processes. RPA can be strongly advocated in business areas ranging from KYC processes and fraud detection to reporting. KYC processes may be manually driven and repetitive but are also critical and mandatory. Setting up, maintaining, and sustaining KYC requires high investment. According to a Thompson Reuters report, the average expenditure of banks on KYC processes amounts to US $380 million annually. Shifting to RPA for KYC would bring down these costs significantly[4]. RPA can collect client data and screen, validate, and process it in nearly 1/10th of the time it would take to do so in a manual environment, at a fraction of the cost, and with much higher accuracy.

Data analytics and data intelligence – Data analytics technologies help field security officers (FSOs) and banks prevent money laundering, fraud, and financial crimes. These solutions can identify new attack and threat patterns, recognize the specific activities associated with these patterns, and adapt their actions to respond effectively to dynamic threats. These technologies are built to take appropriate action when a specific pattern or fraud method is detected. They adapt to these patterns in record time with minimal impact and cost. Data analytics and data intelligence technologies provide high-quality data with a single view of customers, counterparties, risks, threats, and opportunities.

AI/ML – The future of compliance through AI and ML is widely acknowledged. Though nascent at present, the next few months will witness financial services firms employing AI/ML technologies in almost every aspect of their compliance functions[5]. For example, decision trees help firms arrive at faster and more accurate decisions even as they reduce inconvenience and friction for legitimate customers during monitoring and surveillance activities. These tools also help investigators who handle AML, fraud, or screening alerts reduce the noise from false positives[6] It effectively combats alert fatigue or alerts falling through the cracks and directs only genuine alerts worth investigating. The Financial Action Task Force (FATF) report, released in October 2020, highlights the importance of exploring and adopting new technologies. It specifically mentions AI and ML as critical for the effective implementation of compliance requirements during the pandemic. While lauding the benefits of automation and accuracy of AI/ML solutions, the report also cautions on their potential lack of explainability and transparency. Nevertheless, the report provides a substantial case for the adoption of these technologies to improve efficiency[7].

Blockchain – Blockchain is effective at and best-suited to counter cross-industry fraud. It uses a shared distributed ledger as the underlying component that enables transparency to a great extent. The parties in a blockchain transaction can review the actions of the other users and thus easily flag off suspicious and fraudulent transactions. It is also possible to increase monitoring by allowing a regulator to become a node in the distributed ledger[8]. This will support a more proactive and real-time interception of transactions. It can eliminate numerous compliance steps and reduce resolution time considerably. Other features of blockchain also make it extremely suitable as a digital technology for compliance. Smart contracts, inherent in the blockchain ecosystem, can effectively block transactions for counterparties with incomplete or inadequate KYC. These also accelerate process automation to boost efficiency and reduce cost.

Digital Initiative	Description	Benefits
Compliance as a service	Transforming current landscape to SaaS model using Compliance solutions on a Cloud	Potential for TCO reduction APIfication of the Landscape Easier Integration to other digital tools
RPA and Automation	Upgrade to automation tools, Deploy software robots or bots that emulate human action	Streamline compliance functions Reduce operating costs
Data Analytics	Extract intelligence from your data to enable faster and accurate decisions	Integrate and consolidate Data sources to harness the power of data Better and faster decisions
Artificial Intelligence and Machine Learning	Implement better compliance processes by way of aggregation and blending of patterns	Streamline processes, increased transparency and better customer management processes
Blockchain	Enable Distributed ledger technology for better monitoring of fraud and terror financing transactions	Resolve and react faster Greater oversight and faster decisioning

Figure 3 – Digital compliance initiatives and their benefits

The Case for Digital AFC and Compliance

Banks and financial institutions have invested and built a multi-faceted, multi-functional, and multi-dimensional compliance structure over the last few years. These structures were indeed essential to address the challenges of regulatory compliance. But the high pace of technological advancement has caused a perceptible shift in the sophistication of banking products and solutions. It is, therefore, imperative to take a global and holistic view and switch to a new digital spectrum. Investing in the transformation of legacy systems to move towards digitalized environments is the way forward. This will position compliance as a business differentiator and a competitive advantage for banks that successfully migrate to digital compliance models.

About the Author

Anuradha

Business and Technology consulting, Project management, Process and Digital transformation in Banking and Financial Services.

Anuradha has 24 years of experience in Business and Technology consulting, Project management, Process and Digital transformation in Banking and Financial Services. In-depth and rich experience in a wide range of Enterprise products in Retail & Corporate Banking, Risk & Compliance and Transaction Management ranging from Product Strategy to Product delivery and Product Support. Combining wealth of experience achieving business growth, managing teams and fostering strong client relations with a global perspective working closely with clients in various geographies. Her favorite blog topics are trends in retail banking, commercial banking, GRC, fraud management and AML areas.

References

1 'Gary Gensler Confirmed As SEC Chair—Here's What To Expect From The Goldman Banker And Crypto Professor (forbes.com)

2 https://www.mckinsey.com/business-functions/risk/our-insights/derisking-digital-and-analytics-transformations

3 https://www.northrow.com/blog/digital-transformation-meets-regulatory-compliance/

4 https://www.comtecinfo.com/rpa/use-cases-of-rpa-in-banking-industry/

5 https://www.niceactimize.com/blog/aml-the-future-of-compliance-617/

6 https://www.finextra.com/blogposting/19788/its-time-for-financial-services-to-embrace-long-term-digitization-of-anti-money-laundering-systems

7 https://www.fatf-gafi.org/publications/digitaltransformation/digital-transformation.html?hf=10&b=0&s=desc(fatf_releasedate)

8 https://www2.deloitte.com/mt/en/pages/risk/articles/mt-blockchain-in-compliance.html

For more information, contact askus@infosys.com

Infosys®
Navigate your next