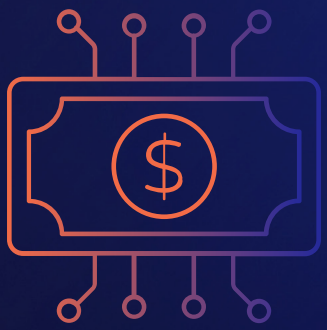
Industry Playbook

FinTech

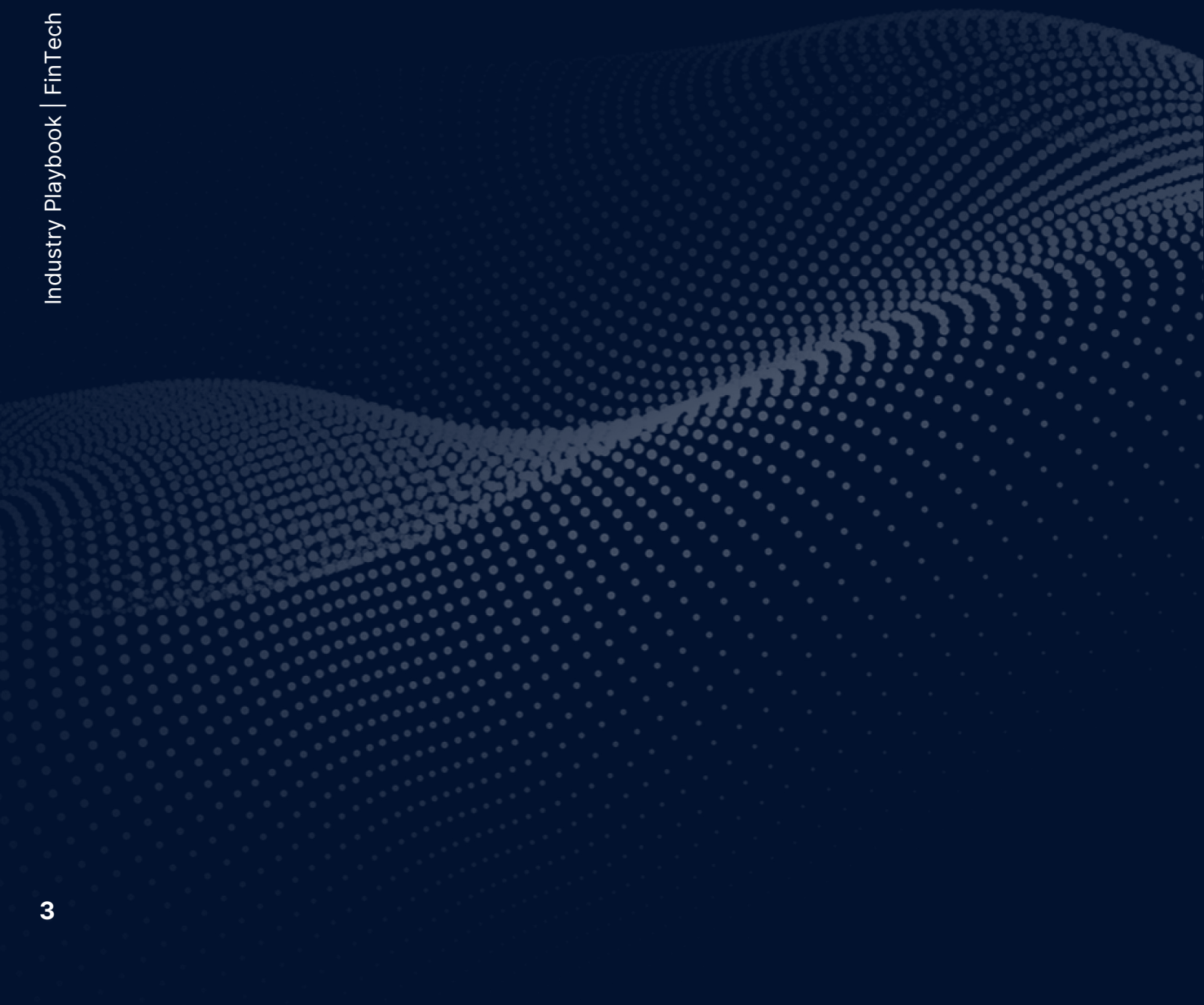


CUBE

Table of Contents

Strategies

for a new era of risk and regulatory compliance in fintech



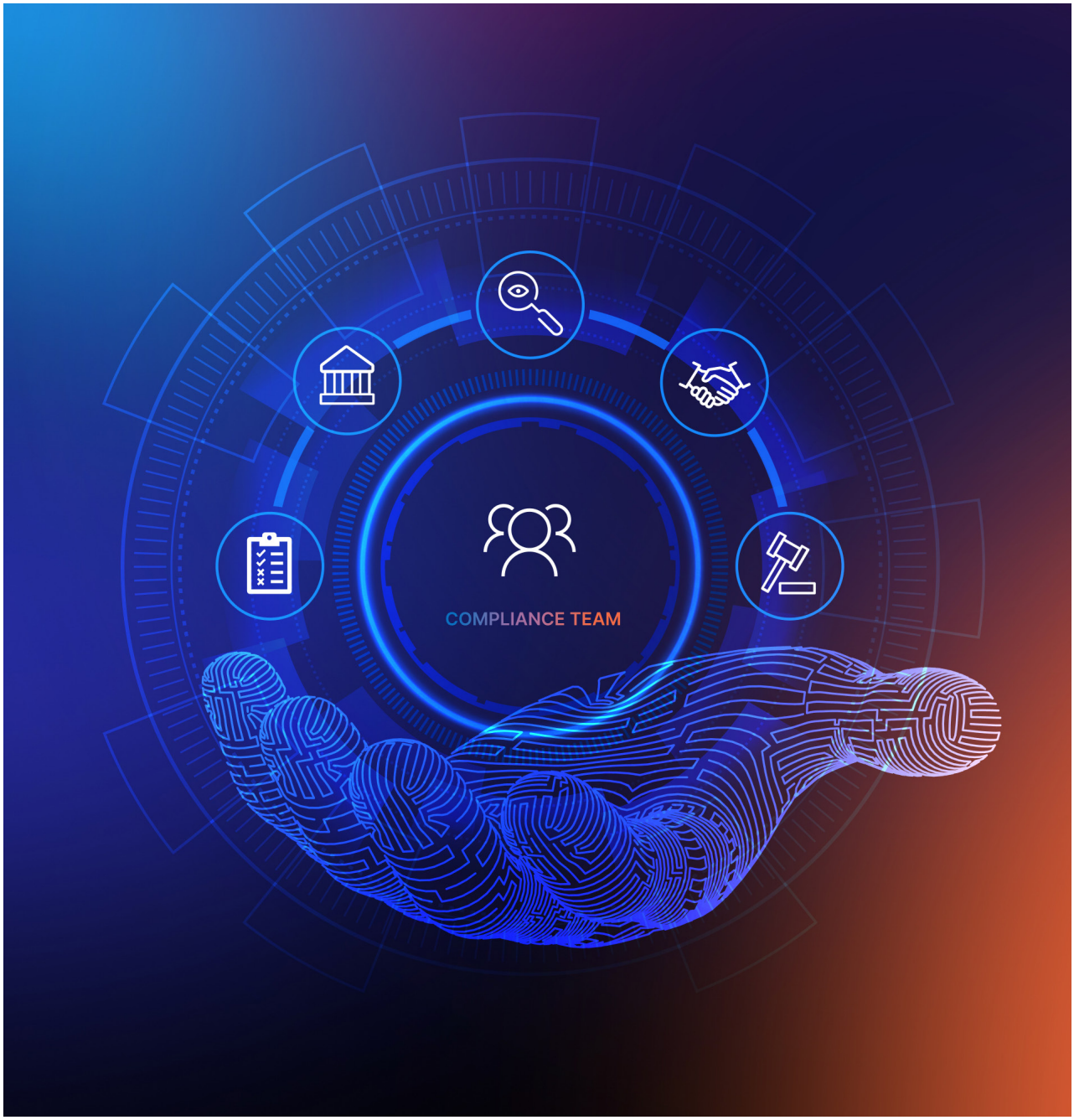
EXECUTIVE SUMMARY

Increased regulatory burdens are inevitable for fintech firms given their growing importance to the sector they serve.

Supervisors probing the financial services ecosystem for weaknesses and areas of risk view the industry's heavy reliance on technology and the speed at which new tools are evolving, as a major flashpoint.

Some agencies believe fintech firms now play a systemically important role[1] in modern finance whereby significant instability could trigger another crisis akin to 2008 if left unchecked.

In turn, the regulatory focus has evolved from a position of observation and guidance to a more interventionist approach.



[1] https://www.fdic.gov/news/speeches/2023/spsept2023.html

EXECUTIVE SUMMARY

Banks will be forced to carry out greater due diligence on their technology partners, and fintechs themselves are increasingly expected to have compliance frameworks capable of meeting requirements on par with large financial institutions.

The days of “move fast and break things” with growth and customer acquisition prioritised above all else are over; compliance can no longer be an afterthought, it is foundational, a necessary platform for growth, and not something that can be built in later.

Without robust, risk-based compliance frameworks in place to account for anti-money laundering (AML), Know Your Customer (KYC), data protection, cybersecurity, safeguarding and resilience, and outsourcing obligations, it will be difficult for fintechs to enter partnerships with banks and impossible to maintain them.

Understanding this differentiator has led forward-thinking firms to deploy Artificial Intelligence (AI)-powered applications across front and back-end operations to help manage regulatory change.

There is clear evidence that leveraging Automated Regulatory Intelligence (ARI) inside the compliance function can help fintechs address the risks on the horizon, continue innovating safely, and make their business more appealing to a potential partner.

It may also appease other stakeholders, such as regulators, consumers, boards, analysts, and rating agencies who recognise the commitment to enhanced risk management practices.

This playbook aims to provide fintech compliance officers (COs) with actionable intelligence, guidance, and best practices to help their organisation harness intelligent solutions to meet the challenges ahead.

The insights contained within have been shaped by users, practitioners, and leading thinkers in regulatory change, and are designed to show how the strategic deployment of AI can significantly enhance compliance operations.

BANKS WILL BE FORCED TO CARRY OUT GREATER DUE DILIGENCE ON THEIR TECHNOLOGY PARTNERS

STEP 1

Act like a bank, think like a bank

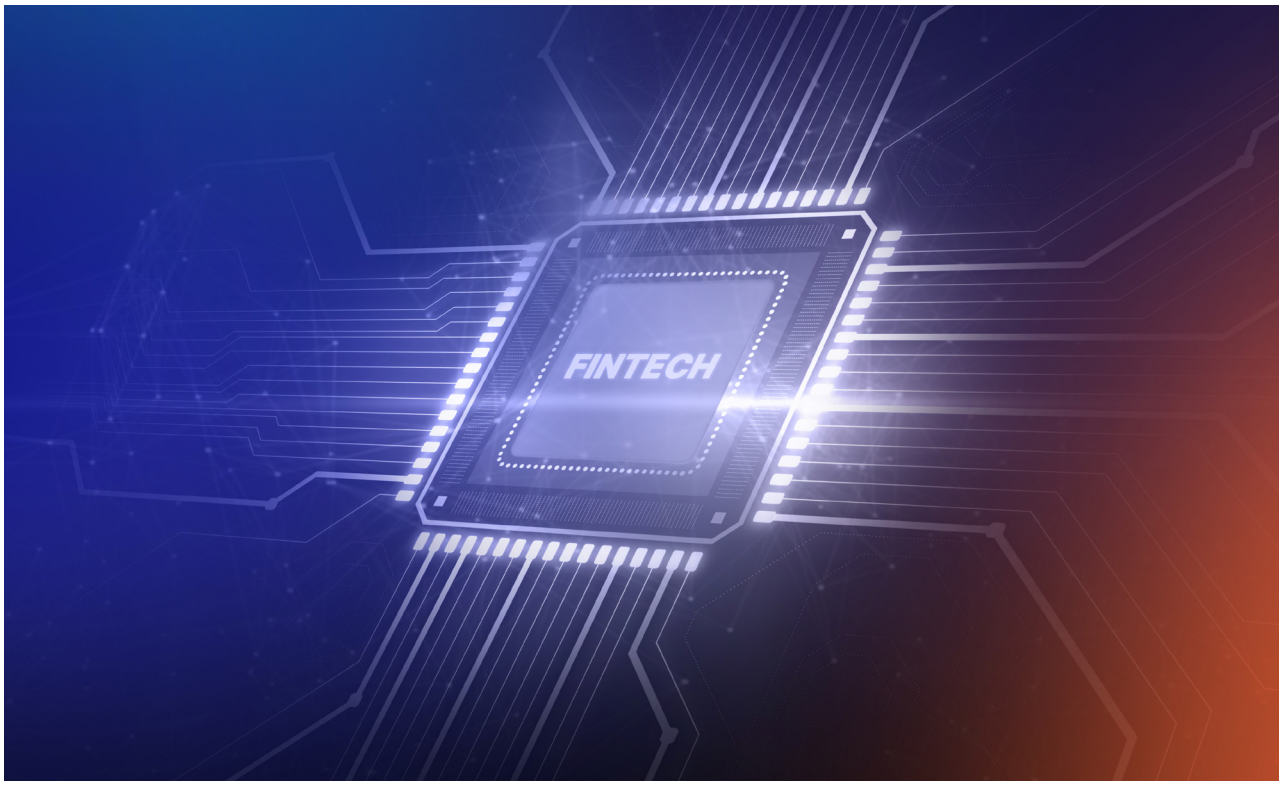
A BRIEF HISTORY OF FINTECH

"Fintech" isn't new. Despite its modern mainstream appeal amongst consumers and investors, fintech can be dated back to the 1850s when telegrams and Morse code helped move money around.

What we know as fintech today has evolved through three distinct eras. The initial wave followed the building of infrastructure that shaped globalised financial services; the first transatlantic cable and Fedwire in the US.

Traditional analogue methods like the telegraph, railroads, canals, and steamships all supported financial interlinkages across borders, allowing rapid transmission of financial information, transactions, and payments across the world.

The 1950s brought about the first credit cards, and non-cash transactions, signalling the end of one epoch and the dawn of Fintech 2.0.



Digitalisation in the 1960s swept in ATMs, before the world's first digital stock exchange, NASDAQ, was established in the 1970s along with SWIFT (Society for Worldwide Interbank Financial Telecommunication), a global financial messaging communication protocol between financial institutions that allowed enormous sums of money to be sent cross border.

Throughout the 1980s, bank mainframe technologies developed and, in 1995, Wells Fargo unveiled the first-ever internet banking product, followed by branchless banking from the likes of ING and HSBC.

Momentum was halted by the 2008 financial crisis, but the global economic meltdown kickstarted the Fintech 3.0 era of start-ups, digital currencies, mobile money and P2P lending. The lack of trust in big banks and the sustained push by international and domestic regulators to introduce more rules in the wake of the crisis resulted in new markets opening and the birth of cryptocurrencies.

The first and still most widely used, Bitcoin, emerged following a famed white paper by an anonymous author in 2008 outlining how a peer-to-peer electronic cash system would solve perceived problems with the financial system.

Blockchain, the technology underpinning cryptocurrency, became a launchpad for startups across the globe who have leveraged distributed ledger networks to provide digitised services and products.

The insatiable appetite for innovation amongst consumers and investors has resulted in banks becoming more like start-ups, pumping billions into product research around distributed ledger technology (DLT), AI and machine learning (ML), and branding themselves as digital-first offerings.

We are now experiencing a Fintech 3.5 where the financial dominance of the Western world has been eroded by advances in digital banking, and particularly in mobile technologies, elsewhere.

Globally, the fintech market is predicted to reach a value of $305bn by 2025, according to Market Data Forecast, driven by rampant consumer adoption and business innovation. Everything from regulatory technology to lending, payments, saving, investing, insurance, robot advice, accounting, risk management, claims processing, and underwriting has a significant fintech element.

The word has become a cliché to describe the activities of the sector, but the disruptive element of fintech's nature cannot be denied.

THE BIG PICTURE: FINTECH SECTOR RISKS

As the historical examples above illustrate, fintech can and often does have a material effect on the structure and functioning of the financial system in both the direct and indirect financing channels. New risks are posed as new opportunities open.

Here are some of the current topics of regulatory concern:

Concentration

The fintech sector is evolving quickly, and specific companies are becoming more concentrated in some areas of financial services and certain geographies.

The underlying economics of intermediation combined with new technology may lead to concentration among both traditional and new financial services providers.

Regulators are probing how best to manage a landscape that is increasingly characterised by new players and business models, and to address potential challenges to financial stability, financial integrity, fair competition, and consumer protection (including data privacy).

Financial stability

Fintech companies that provide core banking functions like credit, liquidity, and maturity transformation can magnify financial stability by diversifying credit and liquidity risk within the financial system.
The newness of the sector and the relative lack of banking experience also opens new entrants to creating systemic vulnerabilities, especially in an economic downturn or during periods of market stress.

The entry of Big Tech into the financial system introduces new risks due to the speed at which they can scale; their intersection with regulated financial entities, and the risks of a few large players carrying out systemically important activities ancillary to financial services, such as cloud services.

Macro-financial

Financial innovations could have the potential over time to produce macro-financial risks that can undermine the stability of the entire financial system. Macro-financial risks might include unsustainable credit growth, pro-cyclicality, and incentives for great risk-taking, contagion, and systemic importance.

Micro-financial

Institution-specific micro-financial risks could have the potential to trigger a situation, which may cause systemic threats.

Managerial

Fintech start-ups which are small often lack managerial capacity, and have fewer financial resources which prevents appropriate scaling, limited credit and start-up experience, lack of a developed business model, inability to deploy analytics and personnel talent, and limited compliance knowledge.

In some enforcement actions against fintech firms, it has been noted that the chief compliance officer (CCO) role is often performed by an individual holding down multiple other positions, some inconsistent with compliance requirements around objectivity. Regulators assessing these risks have taken two distinct approaches to this point. Either existing rules are revised to account for developments, or new legislation is drawn up to promote the development and implementation of new technologies by banks in compliance with the existing regulatory framework (e.g., data protection and privacy).

Aware this may result in a fragmentation of markets and approaches; several jurisdictions are mulling international co-operation on guardrails for fintech firms. This puts the onus on fintech firms to ensure their horizon-scanning capabilities sufficiently capture the incoming wave of regulatory change.

Key takeaway

To understand where fintech is heading, it is crucial to consider the forces behind its evolution, and why regulatory compliance risks are more pronounced now than at any point in the industry's past. The observational, "wait and see" stance of supervisors is giving way to an interventionist approach of guardrails and enforcement.

STEP 2 Broadening horizons of regulatory risk

Over the last two decades, the fusion of finance and technology has delivered an inexhaustible array of products that affect the daily lives of billions of people around the world.

From mobile banking, money remitting apps and a multitude of contactless payment methods to AI stock-picking, lending, invoicing, payroll solutions and more, the use cases continue to multiply.

The ability of fintechs to ease points of friction that consumers have experienced with incumbent institutions has been one of the main drivers of this sustained change, along with the ability to enter markets without the regulatory and legacy headwinds of traditional financial institutions.

Heightened customer demand post-pandemic and the further digitisation of trade have caused a significant blurring of the lines for regulators.

The prevailing view now is that as fintechs provide products and services like the banks themselves, they are also exposed to similar risks, and should be regulated in line with other financial institutions.

For fintechs it means factoring in the ever-changing world of traditional financial services regulation and heavy supervision into strategy, governance, and risk management. Alongside these obligations are issues of growing importance on the horizon related to cybersecurity, data protection and management, outsourcing, and operational resilience.

In the US, federal bank regulators such as the Office of the Comptroller of the Currency (OCC) and Federal Deposit Insurance Corporation (FDIC) have taken great interest in the role fintech firms play in wider financial services, but they do not have the legal mandate to apply bank regulations to fintech entities.

Where they can step in, however, is enforcement actions, particularly if the fintech is considered a service provider under the Bank Service Company Act.

The introduction of a special purpose charter for fintechs has been in the works for several years, and this would give the likes of the OCC regulatory and enforcement authority over firms that opt to sign up.

"Regulatory change management is often not something fintech firms consider given the environment many of them come from where innovation is the central driver. But as they get exposed to the regulatory world of traditional finance and are trying to win deals, that's when things like policy management, training, controls operation and testing start to matter, and where AI can give them a significant advantage." Ben Richmond, CUBE CEO and founder.

UK financial regulators took a similar approach to the regulation of crypoassets and cryptocurrencies; expanding consumer protection mandates to enable them to legally target firms who break rules around promotions even if that firm isn't regulated or even located in the UK.

Concurrent to this and aligned with trends in both the UK and European Union, is the supervisory initiative to investigate banks' third-party service providers, particularly fintech firms.

Broadening regulatory perimeters will continue to create various risk management requirements for fintech firms that compare with those in traditional finance, such as AML, consumer protection, cybersecurity, and data privacy.

Fintechs that adopt a proactive approach to compliance, with the ability to anticipate, identify and head off risks on the horizon rather than react to regulatory updates, stand best placed to succeed.

"As these risks become more apparent and increase with the growth of a fintech company, existing risk management programmes inclusive of compliance, if they exist, will likely need to be revisited or expanded. Notwithstanding that risk management is costly and often not measured in terms of return on investment (ROI), without it a fintech's ability to continue on its trajectory to generate revenues may become inhibited." Peter Reynolds, Managing Director, Deloitte Risk and Financial Advisory.

UNDER THE MICROSCOPE: BUSINESS RISKS

A perfect storm of stratospheric growth, emerging technologies, support and adoption within traditional finance and regulatory interest has made the fintech sector an exciting yet challenging place to innovate.

These forces have exacerbated risk for businesses active in the space,[2] and will fall on CCOs to mitigate by building out a robust compliance framework that broadly covers three aspects of risk:

Operational:

Operational threats can crystallise when outdated or immature processes lead to customer service issues, whilst outsourcing vital controls for cost reasons (e.g., KYC and AML checks), can also magnify risks.

Regulatory:

Suboptimal processes can also lead to regulatory enforcement or litigation, reputational damage, and the loss of business, whilst other forms of non-compliance can result in senior staff being held liable for failures that occurred under their watch.

Financial:

The fallout from these regulatory and operational risks can harm the business by driving away customers, potential partners or acquirers, and cost considerable sums in terms of financial sanctions.

As with their traditional financial services counterparts, how a fintech business manages change and balances rapidly evolving regulatory and business environments is the key to success.

Key takeaway

Regulatory perimeters are widening. Fintechs that adopt a proactive approach to compliance, with the ability to anticipate, identify and head off risks on the horizon rather than react to regulatory updates, stand best placed to succeed.

[2] https://www2.deloitte.com/us/en/pages/regulatory/articles/fintech-risk-management-regulation.html

STEP 3 Developing a robust, risk-based compliance framework

Finance is increasingly borderless thanks to advances in cloud technology, exposing any business that hopes to scale to various domestic and supranational laws and regulations.

For new entrants to the world of financial services, as so many young fintech companies are, the demands can be daunting.

The need for a strong compliance framework is vital; covering policies, procedures, internal controls, incident management, and escalation methods to guide team members.

Banks have built up formalised risk and compliance frameworks over many years, but for fintechs this can be a new experience and one which many now understand is key to their survival.

In the past year, several fintechs have experienced intense regulatory scrutiny and some negative reputational harm, often stemming from operational and compliance weaknesses or failures. An effective, risk-based compliance framework built around automated tools can help protect fintechs from future reputational damage.

The speed of digital innovation requires fintechs to ensure their compliance frameworks stay in step with the regulatory demands that affect processes and products, and the compliance framework itself requires a growth mindset to match.

"For a software company, all of these requirements can be new and confusing. Many software companies are not subject to consumer or financial regulatory requirements; moving into payment facilitation opens up a whole new world of requirements that necessitate implementation of a formal compliance programme," Andrew E. Bigart, partner and regulatory expert at Venable law firm in Washington, DC.

While best practices and regulatory guidelines are readily available for both the qualitative and the quantitative elements of compliance risk, many firms continue to struggle with the practical implementation of these risk frameworks.

Understanding the regulatory environment is a vital part of creating the compliance framework. In an era of heightened risk and scrutiny, staying up to date with the latest regulations and wider supervisory thinking is imperative.

The concept of a robust risk-based compliance framework is one which fintech COs should become familiar with, consisting of a structure and guidelines within the compliance department that enable the department to craft policies which the organisation must follow, and processes to successfully implement legislation.

One of the most significant changes in risk management over the last decade is the need and requirement of senior management and boards to be fully informed of the threats facing their business.

Operational risk events can have catastrophic financial and reputational consequences.

An effective compliance programme should provide foresight of regulatory risk exposure to allow senior management to make strategic business decisions that are fully informed by any risk implications.

An effective compliance programme also provides transparency into threats within the business, allowing for better decision-making. Robust compliance risk frameworks can help fintechs avoid unwanted surprises and arm the business with tools and plans to respond when an event does occur.

External parties are also taking more interest in the operational robustness of a firm, with rating agencies, investors, and research analysts asking for evidence that effective controls are in place.

"Rules-based functions focus solely on the letter of the law and have broad but shallow programmes to track relevant rules, laws, and regulations and test and train for compliance within them. The goal of a risk-based compliance programme is to reduce the overall compliance risk by focusing greater effort on managing the most material risks."
Elena Belov, financial services and organisational effectiveness partner at Oliver Wyman.

BUILDING A RISK-BASED FRAMEWORK

1: Risk assessment and identification

The organisation's operations and activities are evaluated to identify potential compliance risks, which are ranked and prioritised.

2: Regulatory mapping and analysis

Identified risks are mapped to relevant regulatory requirements and industry standards. Gaps between current practices and regulatory expectations are identified.

3: Risk measurement and evaluation

Quantitative and qualitative metrics are developed to measure the level of each identified risk. The potential financial, operational, legal, and reputational consequences of non-compliance are assessed.

4: Control and mitigation strategies

Control measures and mitigation strategies are developed and implemented for high-priority risks. Specific policies, procedures and guidelines are defined to address compliance gaps.

5: Monitoring and reporting

A systematic monitoring process is established to track compliance with established controls. Risk assessments are regularly reviewed, while compliance reports are generated for management and relevant stakeholders, highlighting areas of potential concern.

6: Continuous improvement

Periodic reviews of the compliance framework are carried out while regulatory changes are incorporated into the framework.

7: Audit and assurance

Internal audits are performed to assess the effectiveness of the compliance framework. Results help refine and improve the framework, enhancing overall compliance.

By leveraging advanced machine learning tools, fintech COs have foresight and context into regulatory risks, and can fully automate formerly labour-intensive manual jobs like policy controls and process mapping. Built-in compliance and ARI tools can significantly reduce uncertainty and are becoming integral to threat reduction strategies inside fintech firms.

Key takeaway

Risk-based compliance frameworks reduce overall risk by focussing on managing regulatory change effectively. Fintechs that implement advanced data analytics capabilities into their compliance frameworks create robust defences that better protect their firm in the face of emerging regulatory trends.

STEP 4 From disruptors to disrupted

Supervisors around the world are responding to the growth of fintech in different ways, but most jurisdictions are favouring an approach where existing laws and regulations apply to any business offering the holy trinity of banking services; lending, deposit-taking, and payments.

Regulators in the US are of the view that fintechs should be covered by existing regulation under the principle of "same activity, risk, same treatment". Technology firms seeking to offer banking services must obtain banking licences, via the same criteria as banks, and they must comply with the same regulations.

However, in other jurisdictions like Hong Kong, Singapore and the Philippines, fintech-specific rules have been created such as in the case of digital banks, which must obtain digital-only licences.

The UK and Australia are somewhere in the middle, with transitional arrangements and restricted licensing in the initial phase, as has been the case for cryptoasset businesses.
In areas where there is little to no activity, many authorities have chosen a "wait and see" approach, where small developments are played out under close observation.

"This is particularly important in areas where fintech is creating considerable disruption because of the speed at which it grows and diversifies, and its use by both regulated and unregulated entities in financial services. Authorities should take appropriate steps to strengthen fintech surveillance and ensure they can effectively monitor new developments, identify any risks, and take steps to mitigate against these risks guided by global standards and best practices." Parma Bains and Caroline Wu.

"Impending new regulations will require everyone involved in bank/fintech partnerships to step up their game if they want to continue to operate in a competitive and innovative environment. Banks will need to clearly and proactively share their oversight requirements. They may require everything from financial information, go-to-market strategies, a target customer base, sales plans and compliance plans from potential fintech partners." Laura Spiekerman, co-founder of identity decisioning platform Alloy.

No matter which path is taken, the message from regulators tends to be the same in that they must balance the potential benefits for society against the potential risks to financial stability and market integrity and keep consumers and investors free from harm.

A recent paper by the International Monetary Foundation on regulatory trends in fintech[3] encourages authorities around the world to work closer together to monitor new developments and risks before they crystallise.

The current direction of travel includes a greater focus on application programming interfaces (APIs), cloud computing, and biometric identification. With many fintechs leveraging cloud computing, it is becoming systemically important to the financial system and entering the sphere of financial regulatory supervision.

As banks continue to shift more software and services to the cloud, regulators and central banks themselves will require in-house cloud development or the ability to collaborate with various service providers.

The US Federal Reserve has inspected Amazon's cloud facilities on-site, while the European Banking Authority has published guidelines for cloud outsourcing.

For fintechs leveraging artificial intelligence, machine learning, and distributed ledger technologies, regulatory action has been limited to risk assessments and issuance of general guidance, but that is likely to change in the very near future.

A report by the US Treasury[4] called for "enhanced oversight of the consumer financial activities" of fintech firms and appears to pave the way for a dedicated supervisory framework for bank-fintech relationships.

[3] https://www.elibrary.imf.org/view/journals/063/2023/004/article-A001-en.xml

[4] https://home.treasury.gov/news/press-releases/jy1105

AUTOMATED REGULATORY INTELLIGENCE AND FINTECH COMPLIANCE

it is good practice for regulated businesses to own a list of every piece of legislation applicable to the firm's activities, with COs requiring the knowledge to understand which rules apply, and how the business can ensure its activities remain within the guidelines.

If a CO is unsure what a particular rule is trying to achieve, where it applies, and whether there is a chance of being fined (or worse) for non-compliance, accessing the primary source is the best option.

On top of the key pieces of legislation designed specifically to regulate the financial markets, there are myriad laws and rules which fintech compliance teams must be aware of that affect their firm's activities.

Many of these laws and rules, like the European Union's General Data Protection Regulation (GDPR), come with heavy financial penalties for breaches. Others, like the UK's Proceeds of Crime Act, threaten imprisonment for senior staff who hold responsibility when a serious problem occurs.

Fintechs that operate cross-border must also contend with a colossal amount of overseas legislation which, when taken together, is often much greater and more complex than the laws governing their domestic market.

International business brings contrasting regulatory environments, watchdogs, and expectations; the substances of law and approach to their application can change.

CUBE's research has tracked more than 40m documents issued by banking regulators around the world since the 2008 financial crisis, showing the scale of the task compliance has in making sense of the rules.

Identifying legislation of relevance to the firm (and for which the compliance team is responsible) is an exhaustive exercise. According to the EY Compliance Risk Survey, 63% of organisations consider these essential regulatory mapping protocols a major challenge to achieve.

Some 65% of respondents do not have a centralised repository of applicable regulatory obligations, and 39% of respondents state that no formal training of regulatory obligations is in place.

"A lot of fintech firms don't have legacy systems to contend with, and the more forward-thinking have begun leveraging machine learning to build out their compliance frameworks. The first movers are at the stage where their systems are significantly smarter given the extent of machine learning that has taken place, enabling their compliance specialists to identify and act on risk much earlier." Ben Richmond, CUBE CEO and founder.

Implementation even of parts of Dodd-Frank, Sarbanes-Oxley, the Second Payment Services Directive or GDPR would not have been possible without technological advancements in compliance. The enormous stream of complex regulation and laws that payment providers alone must contend with has made machine learning an essential extension to regulatory monitoring and management.

As boundaries between technology and finance continue to blur and regulatory perimeters broaden, the coming era for fintechs is one where the disruptors are set to become disrupted.

The regulatory focus will centre on compliance and the protection of a fintech's operational, financial, and reputational integrity, which requires an effective, holistic and risk-focussed approach.

Automated Regulatory Intelligence tools can help fintechs navigate this period of increasing regulatory oversight with rock-solid compliance frameworks that give them a platform to mature, grow safely, and continue delivering the innovations which are propelling finance forward.

Key takeaway

Automated Regulatory Intelligence tools can provide real-time horizon scanning of regulatory sources, with powerful machine learning engines able to capture, categorise, translate (where necessary) and explain the relevance of the updates in the context of a fintech compliance framework.

CONCLUSION: HUMAN EXPERTISE AND INTELLIGENT TECHNOLOGY IS A WINNING PARTNERSHIP FOR FINTECH

- The continued importance of technology to financial services is ushering in a new era of regulation aimed at capturing fintech activity and aligning it with the rules in place for traditional finance.
- Intelligent technology is being used to identify and ingest data from a broad range of regulatory channels, giving fintech compliance departments total vision to help guard against emerging regulatory risks.
- Appropriate and effective technology is the best partner to compliance and a strong weapon in the armoury of the business in guarding against risk.
- Machine learning engines can provide real-time horizon scanning of regulatory sources, capture, categorise, translate where necessary, and explain the relevance of the updates in the context of a fintech organisation's compliance framework.
- Automated Regulatory Intelligence can help perpetuate a culture of trust, business integrity, and accountability across the entire organisation.

Fintechs are entering the era of regulation, where an escalation of supervisory expectations will present new challenges for compliance departments.

Dynamic regulatory landscapes bring constantly evolving laws, amendments and industry trends, and the sheer volume of issuances across multiple jurisdictions can be overwhelming for COs to manually track and interpret.

Forward-thinking firms understand the most effective compliance strategy is to get ahead of problems before they crystallise, shifting from a reactive approach to a proactive department capable of harnessing AI effectively.

COs are leveraging intelligent tools to build robust and active compliance frameworks, using AI and automation to help fast-moving, scalable businesses deal with regulatory change management.

The most effective deployment of AI is a synergy of human excellence and machine capabilities, and the fintechs best placed for success are those who combine intelligent tools with a cohesive regulatory management strategy.

ABOUT CUBE

CUBE has been the market-leader in RegTech since the business was formed in 2011. Our unrivalled regulatory change management solutions helping the world's biggest banks and fintech companies, Fortune 500, FTSE companies and leading names in other highly regulated industries solve complex regulatory challenges.

WHERE CUBE STANDS OUT

- Increased agility and capability to manage regulatory change – Make better informed compliance decisions using a complete regulatory inventory.
- Reduce time and costs – save up to 30-40% of compliance costs by freeing up highly qualified individuals from manual tasks to work on valuable operations, analysis, and critical thinking.
- Horizon scanning for compliance – gain oversight over upcoming regulations and plan ahead when it comes to regulatory policies and controls.
- Implement effective, auditable compliance – provide evidence to regulators and internal audit teams across the entire regulatory change process.
- Easy integration into compliance systems and processes – integrate CUBE into your other GRC and risk systems.
- Avoid non-compliance enforcement actions – preserve company reputation and avoid regulatory fines.

ABOUT THIS PLAYBOOK

This intelligent compliance strategy playbook is aimed at compliance and risk professionals responsible for maintaining compliance inside the fintech sector.

Working with our partners, CUBE has developed this guide to support teams considering a move to automated regulatory intelligence technology solutions, which we would be happy to facilitate.

CUBE

Contact

WEB www.cube.global

MAIL hello@cube.global

If you would like to discuss this report in more detail or learn more about how we can help you, email hello@cube.global today.