



Grappling With Financial Services Regulation? Here's How AI Can Help You Comply

Grappling With Financial Services Regulation? Here's How AI Can Help You Comply

Executive summary

Regulation is prevalent in many sectors, but it especially affects the banking, financial services, and insurance (BFSI) markets. Regulators worried about issues including operational resilience and cybersecurity are putting more pressure on these companies to monitor and manage myriad facets of their operations.

Compliance is daunting for many BFSI companies in this fast-moving regulatory setting. They must race to achieve compliance with each new regulatory update, and then constantly monitor their operations to ensure they remain compliant.

To make matters worse, companies in this sector must innovate as they struggle to compete in an increasingly competitive market. This creates tension between compliance teams and business teams when compliance processes cannot keep up with the need for fast development and deployment. Digital transformation demands speed. How can financial companies balance the two competing forces?

Regulatory technology is helping companies to accommodate business needs by streamlining and accelerating the compliance process. It provides a new approach to managing and monitoring the digital infrastructure on which BFSI companies increasingly depend. This white paper will explore the role of the latest technology as compliance pressures increase, and look at how Wipro's Cloud Compliance Shield running in the AWS cloud provides a way to streamline compliance and support growth simultaneously.



A look at the complex BFSI regulatory landscape

Regulation has grown more complex for BFSI companies in the last few years thanks to a tranche of new rules. These include not just generic privacy regulations such as GDPR in Europe and various state-level laws in the U.S, but also finance-specific laws across multiple jurisdictions:

U.S

New York's NYDFS Cybersecurity Regulation went into effect in 2017, imposing strict cybersecurity controls on financial companies doing business in the state.

Consumer financial protection laws have proliferated in the U.S. The Consumer Financial Protection Bureau implemented 18 new rules in its first year alone, compared to 22 rules in the previous administration's [entire tenure](#). Rules such as the Personal Financial Data Rights Rule to promote data portability and support [open banking](#) have placed more pressure on financial companies, as has the amendment to the Equal Opportunity Act to gain more information about [small business lending](#).

UK

The Financial Services and Markets Act 2023, part of the broader 2022 Edinburgh Reforms, severed UK BFSI regulation from the EU to reflect a post-Brexit environment, creating more regulatory complexity for financial institutions.

EU

BASEL III. 2025 will see the EU's new banking package come into force, implementing the [Basel III banking requirements](#). The emphasis is on increasing the resilience of the banking system, and the EU will phase in market risk rules



to support this over time. Other regulations include anti-money laundering rules to [fight terrorism](#).

DORA. The Digital Operational Resilience Act ([DORA](#)) will apply as of 17 January 2025. It is designed to strengthen the IT security of financial entities such as banks, insurance companies and investment firms and ensure that the financial sector in Europe can keep its digital infrastructure resilient in the event of severe disruption.

Asia

Singapore's Technology Risk Management (TRM) Guidelines, amended in 2021, imposed technology controls and incident assessment requirements on financial institutions operating in the country.

Each jurisdiction is imposing plenty of rules in other areas such as open banking, each with its own unique flavors, carrying varying regulatory implications. As each jurisdiction's regulatory requirements grows, so does the complexity for BFSI companies. Yet non-compliance in the face of some regulations can result in stiff penalties, including fines, reputational damage, and business restrictions.



Operational resilience as a regulatory priority

Operational resilience is a big factor in many new regulatory movements, as governments fret about the health of the financial system. The worry is that as BFSI companies become increasingly reliant on digital infrastructure, any disruption to that infrastructure could affect their ability to process transactions, carrying broader ramifications for critical national infrastructure and the economy. From a cyber perspective, financial companies really are collectively too big to fail.

Governments have responded to this concern. In the U.S., the Federal Reserve imposed a rule forcing banks to notify regulators of significant [cyber incidents](#) within 36 hours. Several regulatory agencies also published [operational resilience guidelines for BFSI](#) in 2020, and legal experts are waiting expectantly for more meaningful digital operational resilience regulation.

In the UK, regulators brought operational resilience rules into effect in 2022 that place new requirements on BFSI companies to identify critical business services and manage resilience across them. These include cybersecurity resilience.

The EU has its own [Digital Operational Resilience Act](#) (DORA), which focuses on cyber resilience among banks in the region. It will be fully applied in January 2025 and will impose wide-ranging requirements for managing digital risk.

These resilience requirements are there to allay a variety of real-world risks, including cyber threats. These threats are becoming more prolific and more sophisticated as criminal groups become more organized.

Cloud adoption is on the rise

The concentration on digital operational resilience has coincided with another big trend in the BFSI sector: migration to the cloud. Financial companies need to develop, deploy, and update business services and applications more quickly in the race to be more competitive. This need will increase still further as open banking regulations continue to proliferate around the globe. Demand will be strong to use the cloud for APIs to support free data exchange between incumbent BFSI organizations and fintech companies.

The financial sector has suffered more than

20,000

cyber attacks costing \$12bn over the past 20 years.

[\(Source: IMF\)](#)

84%

of financial services organizations are considering cloud computing.

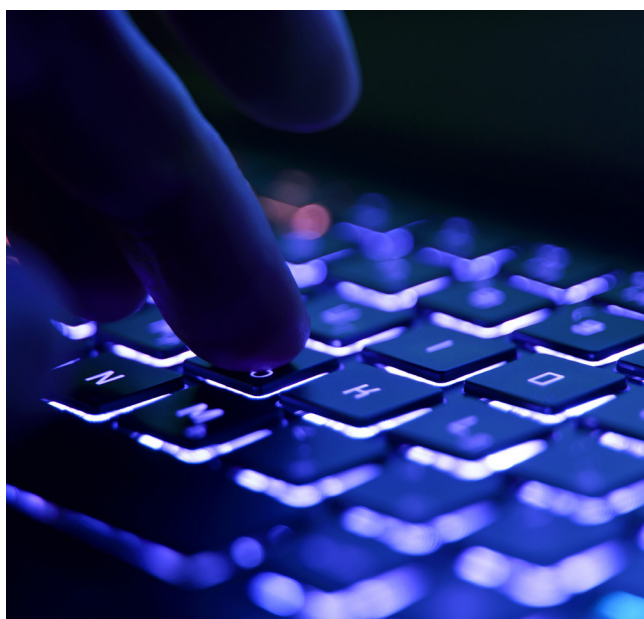
[\(Source: Fintech Global\)](#)

While the cloud offers many benefits for BFSI companies, it also raises its own compliance worries related to digital operational resilience. Regulators have expressed concern about BFSI's reliance on a relatively small number of cloud providers, which they suggest could render multiple financial players vulnerable to common infrastructural risks.

In 2022, the UK's Prudential Regulation Authority (through which the Bank of England Regulates the financial sector) investigated this issue. It led to a 2023 Bank of England policy update requiring financial services companies to assess the risks involve with outsourcing their functionality to third parties including [cloud service providers](#). Rather than slowing adoption of cloud services, this policy update acknowledges the ongoing migration of BFSI functions to cloud environments but demands that financial companies put the appropriate checks and balances in place.

One way to meet these policy requirements is to adopt multi-cloud solutions. This gives financial companies backup processing and storage capabilities in the event of an outage with one provider, increasing operational resilience in cloud environments still further.

Multi-cloud deployments bring complexity challenges. Not only must BFSI organizations manage their infrastructure across multiple technical domains, but they must also manage their data. Data sovereignty is a critical factor in modern business, especially in highly regulated industries like finance. Everything from customer information to payment records must be managed in accordance with jurisdictional rules about where that data can be processed and stored. Meeting those requirements adds yet another layer of complexity to an already complex situation.



The adoption of AI in the BFSI space

The cloud goes hand-in-hand with another promising technology for BFSI organizations: artificial intelligence (AI). Like other sectors, BFSI companies have been inspired by the promise of AI. First came machine learning and its ability to manage tasks ranging from customer segmentation to fraud detection. Then came generative AI, which offers still more opportunities in areas including data ingestion and customer service.

The enthusiastic rush to AI comes with a caveat, however; the possibility of yet more regulation. We have already seen some of this with the advent of the [EU's AI Act](#). This bans some AI systems altogether, and introduces strict risk management requirements for the developers of certain high-risk systems.

AI regulation is still underway in the U.S, while a previously regulation-averse UK has switched course under the new government, which promises to be more hawkish with a bill regulating some of [AI's most powerful models](#).

One common call among ethical AI advocates is the need for explainable AI. Most iterations of the technology are 'black box' affairs that output results without showing their work. Generative AI developers such as OpenAI don't fully understand the inner workings of their [foundational models](#). Yet as organizations in regulated industries like finance use AI to consult on potentially life-changing decisions, it is important not only that they allow human reviewers to assess that input, but also to understand how those decisions were reached to enable proper accounting and discussions with regulators.

43%

of financial institutions say that AI has bought them operational efficiencies.

[\(Source: NVIDIA\)](#)



How AI-powered technology can help

As regulatory complexity rises in step with these emerging technologies, so too does the risk of 'compliance creep', in which BFSI companies struggle to maintain visibility and control of compliance-readiness across large, diverse IT infrastructures such as the cloud, along with AI-driven process flows.

Existing compliance efforts will prove increasingly ineffective in the face of these evolving challenges. They are based on fixed controls and assessments, gleaned manually from documentation issued across multiple jurisdictions. This information takes time to collect, digest, and translate into compliance rules that can be used internally. In short, compliance staff traditionally look at regulations in the rear-view mirror, often having scant time to view the compliance challenges ahead.

Internal compliance controls are also often manual. They have a limited ability to cope with rapidly changing conditions across large numbers of processes and data points. As those data points increase and the processes become more complex and interdependent, it doesn't take a prophet to see the dangers ahead.

Compliance systems need an upgrade. They must become dynamic, adapting to a fast-moving regulatory ecosystem that is running to keep up with a rapidly evolving and diverse set of potential threats. They must also be able to monitor and respond to events on the ground as they happen, alerting the necessary people to compliance creep as - or even before - it happens so that they can respond with appropriate speed and keep their compliance efforts on the rails.

The growth of regulatory technology

Regulatory technology is attractive for BFSI companies as grappling with outdated compliance processes. It automates aspects of the compliance process with AI's help. AI excels at managing complexity, especially in volatile operating environments. Its capabilities map perfectly to the digital resilience problems facing modern BFSI companies, and these abilities promise to propel the category's projected growth in the next few years.



BFSI companies can use AI-powered technologies to build dynamic compliance frameworks and strengthen their cybersecurity measures. A dynamic compliance framework automatically tracks regulatory changes across multiple jurisdictions, ensuring that a company works in line with the most current regulatory requirements. Its internal monitoring controls also keep a company operating in line with those requirements.

Technology solutions for the management of regulatory processes, especially those powered by AI, bolster BFSI organizations' compliance capabilities in several areas:

Operational resilience

Help support comprehensive risk analysis and incident response planning.

Data sovereignty compliance

When hosted in the cloud can assist BFSI companies in ensuring compliance with local data residency requirements, maintaining data localization without sacrificing cloud resilience or scalability. This helps them comply with international data protection laws.

Compliance automation

Makes a BFSI organization more agile in adapting to legal changes, because it proactively monitors the regulatory landscape for alternations and updates.

Transparency and accountability

Sheds light on how decisions were made in a complex organizational environment, which is a critical tool when justifying those decisions to regulators. AI awareness in modern solutions gives BFSI companies access to explainable AI, supporting these needs.

Revenue from technologies used for the management of regulatory processes within the financial industry.

will increase at a

20%

CAGR from \$83m in 2023 to \$207m in 2028.

[\(Source: Juniper\)](#)

Continuous improvement

These technologies do more than keep companies on the right side of the regulatory line. They also support continuous learning programs by enhancing the understanding of compliance requirements among the compliance team and the IT team alike.

The AWS-powered Wipro cloud compliance shield

The Cloud Compliance Shield is Wipro's response to the compliance challenge facing BFSI organizations moving to the cloud. Powered by Amazon Web Services (AWS), this system uses AI to monitor compliance across multiple cloud environments, ensuring that BFSI organizations meet their regulatory requirements while taking advantage of the cloud's resilience and flexible computing advantages. It offers several key benefits:

Automating regulatory updates

Finding and analyzing new regulatory information across multiple jurisdictions is a burdensome task that has traditionally taken weeks of manual work. Wipro Cloud Compliance Shield's generative AI capabilities automate this process, gathering new documentation and analyzing it with precision before mapping this information against BFSI companies' internal controls.

Stronger compliance visibility

As an AI-powered solution, Wipro Cloud Compliance Shield uses cutting-edge generative AI capabilities to help solve the compliance challenge. GenAI creates an intuitive interface to help query the cloud-based service about any aspect of a financial company's cloud compliance stance, producing answers in an easily digestible form. Wipro uses Amazon's Security Lake as the source for this comprehensive infrastructure data, which is updated in real time.

Continuous monitoring

After digesting and mapping the latest regulatory changes, Wipro Cloud Compliance Shield continuously monitors the cloud computing and data infrastructure. This ensures that BFSI companies follow controls across a complex IT landscape that spans multi-cloud environments, on-premises data centers, and colocation facilities. This automated monitoring, along with its alerting and reporting capabilities, prevents compliance creep by highlighting problem areas for remediation quickly and accurately.

Fast, accurate risk assessment

Wipro's AWS cloud-based solution is an excellent risk management platform, using its AI capabilities to highlight areas of concern to compliance and risk managers. It helps BFSI

organizations identify areas where digital operational resilience efforts might drift outside best governance practices.

Fast, accurate cybersecurity remediation

The Cloud Compliance Shield's real-time view of compliance and security posture across a BFSI customer's entire environment enables it to quickly identify security misconfigurations and alert administrators. Together, Wipro and AWS maintain a robust inventory of data held in a BFSI customer's IT infrastructure.

This data set, which is constantly updated, enables the Wipro Cloud Compliance Shield to highlight any potential data sovereignty compliance issues and recommend mitigations. Those recommendations take other compliance requirements into account, ensuring that any changes to data structure maintain digital operational resilience for financial firms.

AI accountability

Wipro Cloud Compliance Shield's underlying AI capabilities rely on Amazon's Bedrock managed AI service. This provides access to foundational models from various large language model providers, offering pre-trained augmented models for specific tasks. Wipro uses this platform to deliver explainable AI-powered compliance recommendations, rendering operational decisions transparent to regulators.

Scalability

One of the cloud's biggest benefits is its ability to scale. BFSI organizations can use this to quickly deploy and grow projects after they have proven themselves at the concept stage. Wipro Cloud Compliance Shield enables them to scale at will without worrying about potential compliance risks, as this solution was designed to support cloud-based applications and data structures.



Manual compliance workflows

Compliance in the BFSI sector extends beyond gathering the appropriate regulatory documentation. It also involves mapping that information against a BFSI's current operations and conducting a gap analysis for compliance updates. Then, the financial company must make the necessary remediations and check to ensure that they are now in compliance. This process repeats regularly in a constantly changing regulatory environment, and each compliance update can take up to four months when completed manually.

Time frame	Regulatory task
4-6 weeks	Gather the documentation
1-2 weeks per regulation	Digest and analyze the control requirements
2-3 weeks per regulation	Conduct a risk assessment
1 week	Research internal compliance stance against documentation
1 week	Report on these findings (gap analysis)
1-2 weeks	Remediate
1 week	Recheck compliance

[\(Source: Wipro\)](#)

Wipro Cloud Compliance Shield removes most of this manual work. Its AI-driven automation turns a lengthy, cumbersome process into an automatic real-time workflow, ensuring that BFSI companies stay constantly compliant.

Wipro and AWS: A strategic partnership

Wipro Cloud Compliance Shield would not have been possible without the strategic partnership between Wipro and AWS. The two companies have a long-standing relationship, supported by a business group within Wipro that is dedicated to maintaining and evolving that partnership. This has helped Wipro to gain high-level AWS partner accreditations. It is an AWS Level 1 Managed Security Service Provider (MSSP) and AWS Security Competency Partner, and it has a decade of experience as an AWS Premier Consulting Partner.

Wipro bought 12 AWS competencies and over 4,500 AWS certifications to bear in the development of Wipro Cloud Compliance Shield. It drew on its deep experience with AWS, including its creation of over 40 AWS solutions serving over 250 partners. This positioned it well to work with AWS in creating a solution with a broad reach into all aspects of cloud compliance and a deep focus on operational risk management.

Cloud compliance as a basis for innovation

All too often, companies view regulatory compliance as a form of tax - something to be shouldered as a cost of doing business. However, streamlined, AI-powered cloud compliance solutions enable us to view it another way, as an opportunity for growth and innovation.



In this context, the Wipro Cloud Compliance Shield is a powerful strategic tool to increase competitive advantage.

Cloud compliance is particularly empowering in digital transformation, which is an initiative that most BFSI organizations are currently tackling. An automated, constantly updated compliance framework frees financial companies to navigate the complexities of digital transformation safe in the knowledge that they are staying inside regulatory guidelines. They can dedicate more resources to creating powerful new customer experiences powered by cloud and AI technologies.

A strong compliance framework also makes it easy to expand geographically, because it gives BFSI companies the confidence to navigate jurisdictional regulations with ease. These capabilities directly support the creation of new revenue streams that would be far more difficult with a manual, reactive, and static compliance process.

Wipro Cloud Compliance Shield also transforms compliance challenges into strategic advantages by enabling BFSI organizations to make operational improvements as part of their regulatory response. Interpreting real-time data from the Amazon Security Lake facilitates enhanced cybersecurity measures that result in real risk reduction. Monitoring controls across the organization empowers BFSI companies to improve operational efficiency and manage costs.

Automated cloud compliance not only reduces cost by minimizing non-compliance penalties, but it also boosts customer trust. It builds confidence in financial companies at a time when customer loyalty is at an all-time low and every brand advantage counts.

[Read more](#) about how AWS and Wipro Cloud Compliance Shield can help BFSI companies to get in compliance and stay there, paving the way for innovation and growth.



ABOUT WIPRO AND AWS

Together with AWS, Wipro helps enterprise organizations thrive by solving complex business challenges with cloud-led, sustainable solutions designed and tailored to customers' unique needs. Transitioning to the cloud enables business agility, improves operational efficiency, and opens new opportunities for innovation and growth. Wipro's deep industry expertise, domain knowledge, technical prowess and innovative services combined with AWS's cutting-edge cloud infrastructure and solutions has proven time and time again to help elevate businesses to new heights in the dynamic world of cloud computing.