
LTIMindtree
PoV
Turning Banking Regulatory Hurdles into Strategic Advantages
A Data and Controls Driven Approach to Remediation

Banking breaches have been a catalyst for regulatory evolution

The banking industry has faced a few devastating breaches, causing chaos both nationally and internationally. These incidents have resulted in billions of dollars in losses, damaged reputations, and, most critically, a decline in customer confidence in the banking system. History has shown us numerous tricks and catastrophes, leading to the development of regulations and regulatory bodies. Even today, these regulatory requirements continue evolving, emphasizing the need for effective remediation in banking operations.

Sr.No.	Organization overview	Year	Type of breach
01	North America based Financial Corporation	2019	USD 885 million financial and personal records linked to real estate transactions were exposed through a common website design error
02	American credit information company	2017	147 million customers' data theft
03	Card processing and e-commerce payment-accepting company	2008	130 million debit and credit card numbers and physical theft of servers
04	Credit financing company	2019	100 million credit card applications containing Social Security Number (SSN) and bank account details

Source: 10 Biggest Data Breaches in Finance, Edward Kost, Upguard, April 21, 2024[i]

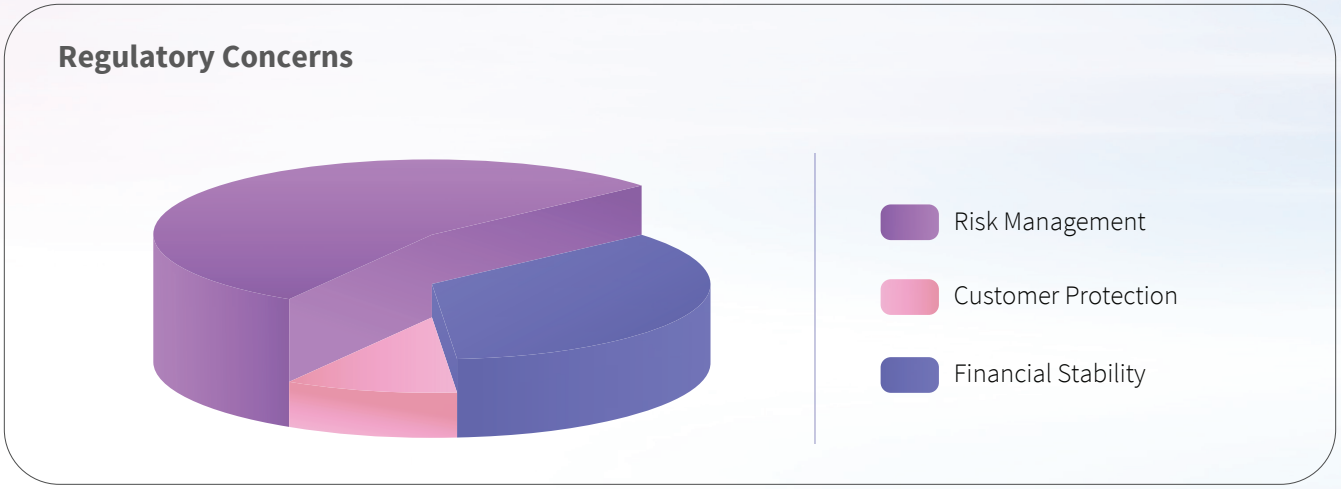
Sometimes, the question remains the same, but the answer changes with time, the nature of business, and the evolution of technology. The same is happening in the banking industry. The industry is witnessing newer risks and opportunities with changing times, especially with fintech integration and banking.

The need for regulatory compliance

The need for regulatory compliance and remediation services in banks was born out of the desire for stability, protection of customers, and, most importantly, repercussions of various financial crises and economic changes.

Evolving regulatory concerns

With the changing trends, today's regulators' concern areas have been–corruption, cybercrime, terrorist financing, fraud, transnational criminal organizational activities, drug trafficking and human smuggling, and proliferation financing. All the above can be assimilated into risk management, customer protection, and financial system stability, which are the primary concerns of the overall regulatory frameworks. The order of priority of these may be articulated as follows:



Increased scrutiny and regulatory perimeter expansion

Going by the fine print, regulators have given enough signals for increased scrutiny of financial institutions in 2024 and the years to come. Larger banks and tier 2 and 3 should prepare themselves for new debt, liquidity, and capital requirements regulations. The intent is to improve governance and risk management. A step ahead, non-banking organizations like fintech, payment companies, and big tech firms like Google and Apple are offering financial products. This leads to the need to increase the regulatory perimeter.

Impact of Basel III and cybersecurity outlook

In addition to any other regulation, the Basel III[ii] international standard will be finalized in 2024. This standard will discuss long-term debt requirements for banking organizations, among other points. The regulatory changes are anticipated to be most consequential for the industry in more than a decade, bringing even mid-size and smaller institutions under the ambit of these regulations. Another document worth mentioning is the World Economic Forum's Global Cyber Security Outlook 2024[iii], which discusses the industry's trends, issues, and cyber inequities.

Addressing legacy issues and new governance

As regulatory scrutiny intensifies, financial institutions need more resources to address legacy issues and build new governance and risk management frameworks. They will also have newer agendas related to resolution planning, consumer compliance, supervision, and changes in capital structure, to name a few. The other tip of the iceberg is evaluating new banking regulations for their impact on existing business models and strategic planning.

Regulators are poised to consider newer technologies and their impact on present operational systems. The deployment of emerging technologies like blockchain, distributed ledger technology, and artificial intelligence is likely to come under increased scrutiny from regulatory bodies. Remediation technology solutions for banks can play a pivotal role in ensuring compliance and efficiency in these areas.

Regulators will focus on consumer protection and the adverse effects of new technologies on safeguarding consumer interests. The industry can anticipate regulations related to fair lending practices and open banking solutions, to name a few. Banks and non-banking organizations can be evaluated for their transition to technological usage and steps taken to guard customer information.

Challenges of regulatory compliance

At times, regulatory requirements play a hurdle to the day-to-day operations of banks in general. One of the challenges banks face is tracking the regulatory obligations concerning the associated processes and controls. They require an enormous amount of data and documentation related to policies and then to update the bank's processes, controls, and policies as per the regulatory requirements. Despite doing this, the fear of heavy fines looms if any non-compliance is proven.

The other hurdle is the compliance cost, especially for smaller banks. The cost related to these compliances may not be one-time. Over a while, the compliance cost may be too high. There have been instances when banks have preferred to close or transfer their business operations from one location to another to save on compliance costs immediately and avoid fines from a long-term perspective. Remediation technology solutions for banks can help mitigate these costs by improving efficiency and reducing manual processes.

Compliance costs vary from smaller to larger banks. Economies of scale play a large role in this. The average compliance cost for a bank with less than 1 billion assets is approximately 10-12% of the retail deposit operating expenses, whereas the same stands at 5-6% for banks with assets of 1 billion to 10 billion.

Compliance cost data is available mainly for American banks only. Based on the information gathered, the mean compliance costs as a percentage of no-interest expenses of all community banks are shown as follows:

Source: Compliance Costs, Economies of Scale and Compliance Performance: Evidence from a Survey of Community Banks[iv]

Another pain point for banks is managing the regulations for outsourced or third-party vendors' activities. Checking and evaluating third-party compliance can be risky despite close monitoring. However, one option is to include compliance requirements in the vendor contracts and transfer the regulatory fines back-to-back.

Training and educating employees about the changes in regulatory requirements is also cost-intensive and resource-intensive. Creating newer competencies based on the changed regulations has posed severe problems to banking operations.

Criticality of regulations for the industry

While discussing the hurdles of regulatory requirements in banking operations, it is also necessary to discuss the importance and relevance of regulations for the industry. Regulatory compliance in banking helps to fulfill local and international compliance regulations. There are legal requirements set by governmental and international bodies which must be complied with. The other relevance of regulations is to manage risk. Banks must manage risks effectively, be it credit risks, market risks, or operational risks. Another intent of regulations is customer protection. Banks and financial organizations are expected to protect customers against fraud, malpractices, and discrimination. Regulations help banks to fulfill these obligations. The other underlying requirement of regulations is to create a stable financial system with adequate capital, liquidity, risk aversive, transparency, ethics, and clear communication about fees, interest rates, etc. A system that builds trust amongst the customers that it will not be affected by financial crises and economic downturns and protects the customer's rights and their personal information.

To prevent money laundering and fraud within the banking system, regulatory compliance measures safeguard both banks and customers from unwittingly participating in illicit activities. This ultimately secures banks' reputation in the eyes of the law and customers alike while ensuring protection at the investor level through compliance regulations.

Opportunities often arise from disasters. In the same way, let's view regulatory hurdles as potential advantages, finding the benefits within the challenges. Today's regulatory obstacles could become tomorrow's business opportunities.

Case in point

Consider the European Union and the current focal point of discussion – the Digital Operational Resilience Act (DORA). The EU aims to achieve seamless banking services across its member states, allowing customers to bank in any member state just as they do in their own country.

Implementing it will be a challenge as the EU will take cognizance of the rules of all member states. The banks will have to comply with EU regulations and also their country regulations. However, all member states will have similar banking regulations sooner or later. This is a problem for the banks in an immediate sense. At the same time, it opens a plethora of opportunities for each bank by increasing their customers in other member states. Hence, this is an implicit invitation to all the banks to extend their operations in different member states.

Banks fulfill their compliance obligations on centralized Governance, Risk, and Compliance (GRC) functions. Other functions are disconnected, resulting in GRC working in a silo mode, detached from banking operations and business risks. Ultimately, compliance management activities lack integration with the broader risk management processes of the bank. Compliance management is not linked to the bank's decision-making process. Instead of using a preventive defense approach, compliance is considered a necessary evil and after-fact activity. Coming back to risk management, it is done as financial risk, operational risk, and Sarbanes-Oxley (SOX) risks in silos, disconnected from one another. Here are the top five factors to turn regulatory hurdles into strategic advantages.

Enhancing risk management through compliance integration

New regulatory requirements encompass the overall risk management process with compliance by integrating the risk management frameworks. This makes the regulatory mandates accessible and understandable to all stakeholders within the bank. It helps create, design, and implement appropriate risk governance, assessment, monitoring, and testing approaches across all lines of businesses of the bank. All risk-related data is assimilated, and the information is presented cohesively while adhering to the new list of regulatory requirements.

Bridging the compliance skills gap in banking

Another hurdle for banks is to get skilled resources for compliance management. Generally, compliance staff is engaged from the legal domain, working in an advisory mode, without having hands-on experience in banking risk management and banking operations. With the new regulatory requirements, operational and technical teams will be equally involved in compliance activities. With this, the present crunch for compliance-related resources will be reduced in the coming times. The main reason will be that banking creates compliance competency from their existing operational and business staff. This will reduce compliance talent scarcity, staff poaching, and costs for the banking industry.

From tactical workarounds to holistic solutions

Until now, banks have taken a tactical workaround approach for technology to meet compliance requirements. With newer regulations, banks have just developed or purchased new micro solutions for managing specific regulatory requirements. With the passage of time, this has resulted in duplication of data, documentation, and processes. Today, banks lack a single source of truth for their information. With the new regulations and the need for remediation technology solutions for banks, there is bound to be holistic involvement of various verticals within the bank. It will bring about more cohesion in data management and usage. Single-point applications will be transformed into more holistic and all-inclusive. The result perceived is saving time and financial resources in the long run.

Automating data management

Regulatory requirements will also bring more automation to the banks, enhancing remediation in banking processes. There is still a reliance on manual files, which are labor-intensive and prone to errors. Being manual, the information is stored in different verticals in different formats and ways, which lack standardization. Sometimes, the tools used are semi-automated and unsophisticated. It is expected that these issues will be resolved in a phase-wise manner with increased regulatory requirements. Hence, banks will achieve more effective remediation in their operations.

Standardization of processes

The regulatory and compliance requirements will also pave the way for the standardization of the testing procedures. The present test in silo for each line of business will give way to a standardized process within any banking organization.

With the regulatory requirements, sub-optimal data governance, aggregation, and architectural processes will be more streamlined. This alignment will ensure coherence between compliance requirements and data origins, enhancing data accuracy and consolidation. Incomplete processes within the organizations will give way to more robust and resilient frameworks.

Conclusion

Needless to say, banks are fined billions for defaults on regulations and compliance. Barring initial tumultuous times, banks will be more resilient, save on the fines, and improve their reputation for compliance through remediation services in banking, reducing any breaches with time.

Going forward, regulators will likely continue to stress Anti Money Laundering, stability in the banking system, debt and cash management, currency management, settlement systems, money regulation, cross-border transactions, foreign exchange, government security market, and financial directives. Compliance costs and expenses will also be directed at these only.

Regulatory priorities are bound to be redefined now and in the future. Banking leaders should continuously analyze the impact of emerging trends and external factors. They must constantly study potential change, its effect on business and operational structures, and regulatory change processes.

References

(i) 10 Biggest Data Breaches in Finance, Edward Kost, Upguard:
https://www.upguard.com/blog/biggest-data-breaches-financial-services

(ii) RCAP on timeliness: Basel III implementation dashboard, BIS:
https://www.bis.org/bcbs/implementation/rcap_reports.htm

(ii) Global Cybersecurity Outlook 2024, World Economic Forum:
https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

(iv) Compliance Costs, Economies of Scale and Compliance Performance: Evidence from a Survey of Community Bank:
https://www.communitybanking.org/-/media/files/communitybanking/compliance-costs-economies-of-scale-and-compliance-performance.pdf?sc_lang=en&hash=19C682B5EFB86B37D6A8604DE9087DA6#:~:text=In%20other%20words%2C%20the%20compliance,by%20year%20in%20the%20study

Author Bio

Neeraj Benjamin,
Lead, Financial Services Risk,
Compliance & Cybersecurity Strategy, LTIMindtree

Neeraj is a risk and compliance advisory leader within the BFSI sector. He provides consulting services in security operations and regulatory standards set by authorities such as SAMA, DORA, IRDAI, and RBI. With expertise in ISO27001 and NIST frameworks, Neeraj conducts comprehensive IT security audits, identifies gaps, and evaluates third-party risks. He has been guiding European and Middle Eastern banks and financial services clients through regulatory compliance complexities. This includes a holistic approach from documentation to implementing security controls, driving client success.

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 84,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — solves the most complex business challenges and delivers transformation at scale. For more information, please visit https://www.ltimindtree.com/.