

# Operational Resiliency and Data Privacy in Financial Services

Restructuring the Business in the  
New Reality

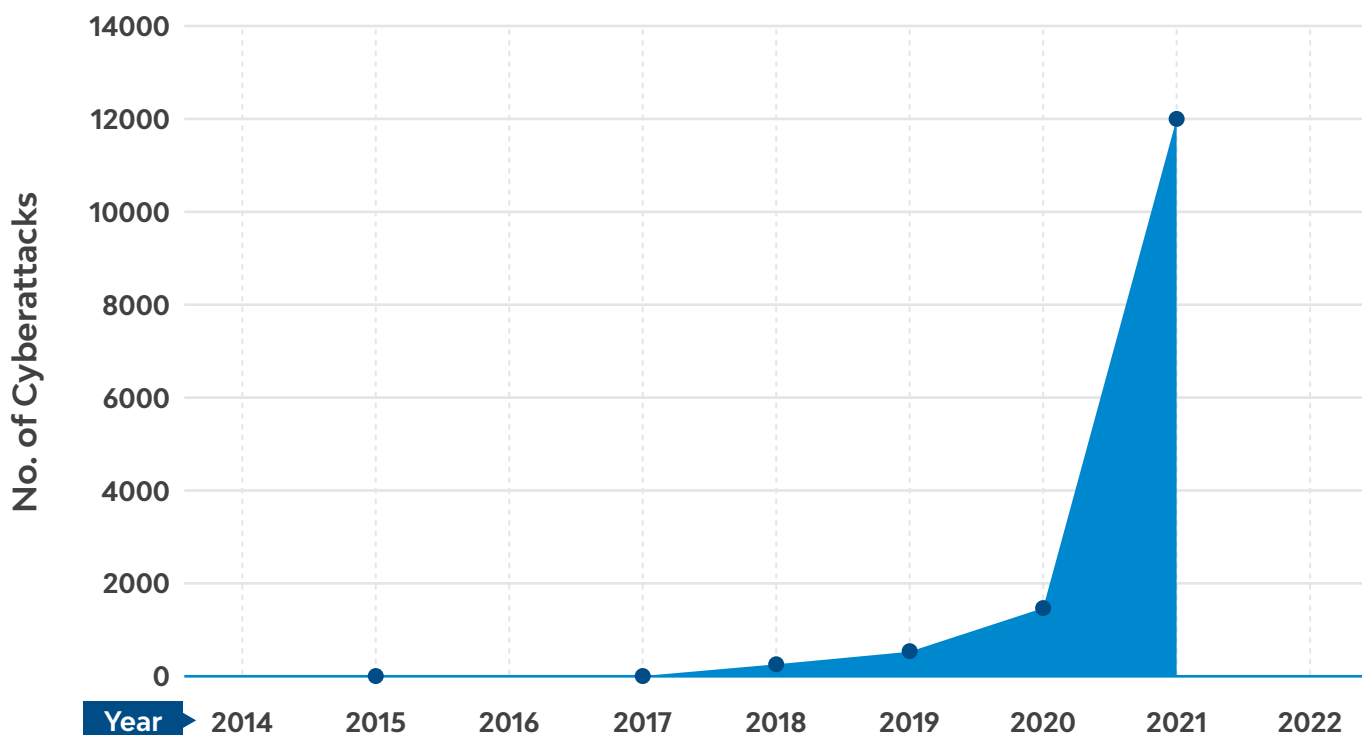
# Background

Operational Resiliency is always a key focus area for any bank/financial services providing organization for its smooth operating. The ability to resist, absorb, and recover from an adverse occurrence ensures that business is continuously operational in challenging times. In this subject, data protection/privacy initiatives are very important from a business continuity perspective.

We have seen a sharp rise in cyberattacks on financial firms in the last few years, especially since the beginning of the Covid-19 pandemic. Many financial firms have been impacted by Information Technology (IT) and Data Privacy challenges during the pandemic. As financial services organizations' dependence on IT grows day-by-day, policymakers across the globe are revisiting the current regulations in order to make them more robust, and drafting new regulations around the operational resiliency of financial firms.

## Next-generation software supply chain attacks in the last seven years

Dependency confusion, typo squatting, and malicious code injection



The increase in cyberattacks year over year (2020-2021) is **> 600%**

# Cybersecurity and Data Privacy Key Regulations- A Global Wave in Recent Years

Globally, lawmakers are taking multiple initiatives to keep the business environment smooth and healthy in their region.

## **Below are some key efforts in brief:**

In 2020 alone, over 280 cybersecurity bills and resolutions were introduced by US policymakers.

### **California Consumer Protection Act (CCPA)**

Essentially, it is intended to enhance privacy rights and consumer protection. In November 2020, California voters passed Proposition 24, also known as the California Privacy Rights Act, which amends the CCPA and makes it further robust.

### **General Data Protection Act (GDPR)**

The GDPR, data protection rules are mainly about data collection and transparency for any organization. It is largely made for an organization that is collecting data from a EU citizen irrespective of that organization's location. This regulation became a model for many other laws across the globe. Countries like Turkey, Mauritius, Chile, Japan, Brazil, South Korea, Argentina, Kenya, and India have similar regulations inspired by GDPR. In 2021, The European Commission introduced changes to the GDPR that are intended to further enhance the effectiveness of this law.

### **Internet of Things (IoT) Cybersecurity Improvement Act**

It is being observed that connected smart devices are potentially more exposed to cyber-attack. Considering the vulnerability factor, US Federal government has established the IoT Cybersecurity Improvement Act. Essentially, this act establishes the security standards for IoT devices owned or used by the Federal government.

## State and Local Cybersecurity Improvement Act

Fundamentally, the Act was referred in the US senate in 2021. This bill requires the Cybersecurity and Infrastructure Security Agency (CISA) to determine and address cybersecurity risks and threats to the information systems of state, local, or tribal organizations.

## Digital Operational Resilience Act (DORA)

Essentially, EU legislation is coming into effect in 2023. The purpose is to provide a framework to financial services organizations in order to operate resiliently in face of cyber threats so that business continuity will be assured in case of potential business disruption.

## Financial Conduct Authority (FCA)

The UK is working on new operational resilience guidelines. These guidelines are likely to be effective by 2024.

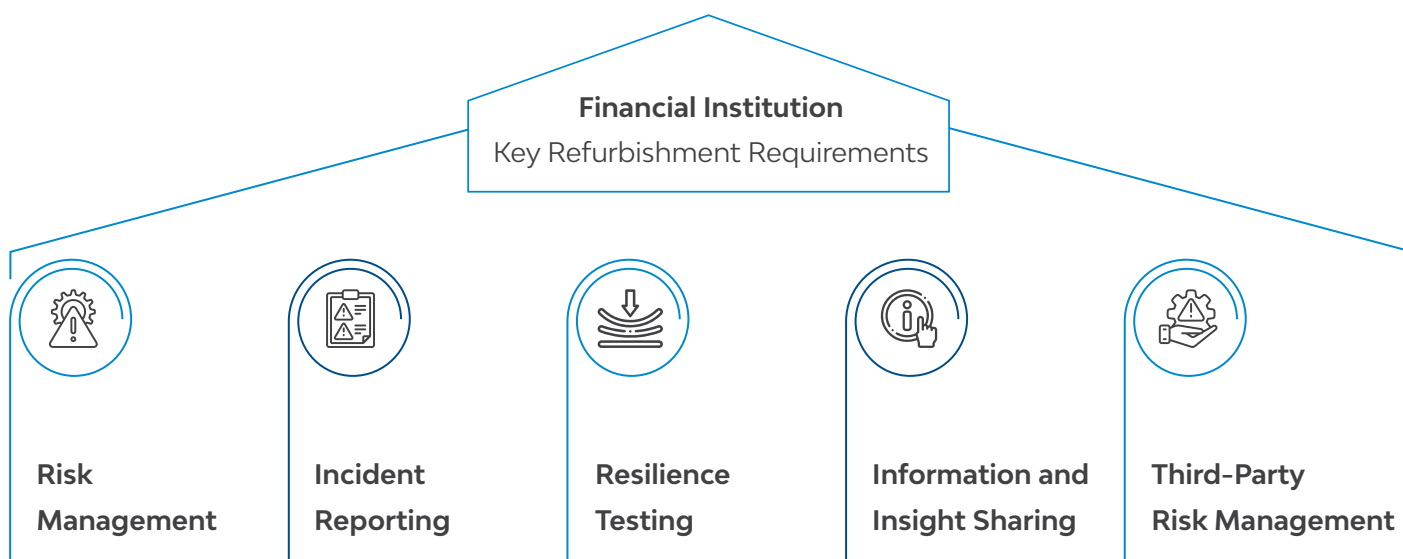
# The Impact on Businesses and Technology

Data security is not only influencing the financial services business, but also its IT ecosystem.

According to Boston Consulting Group (BCG), financial firms are 300 times more likely to experience a cyberattack in one form or another compared to other institutions. The pandemic has shown a surge in the usage of self-service and contactless banking. Financial institutions' clients have rapidly adopted mobile wallets and digital banking options rather than visiting the branch in person.

The fast-growing self-service technology uses artificial intelligence and machine learning to help clients make financial decisions. These applications are creating risks due to implanted open-source components. We can see financial organizations' large dependence on using third-party services like cloud, remote data centers, software, data analytics, etc. Financial firms are revisiting their contracts with IT and third-party suppliers. Information on data storage, location, data usage, personal data security, and service level agreement are the key areas that need to be revisited and compliant with the recent and upcoming regulations.

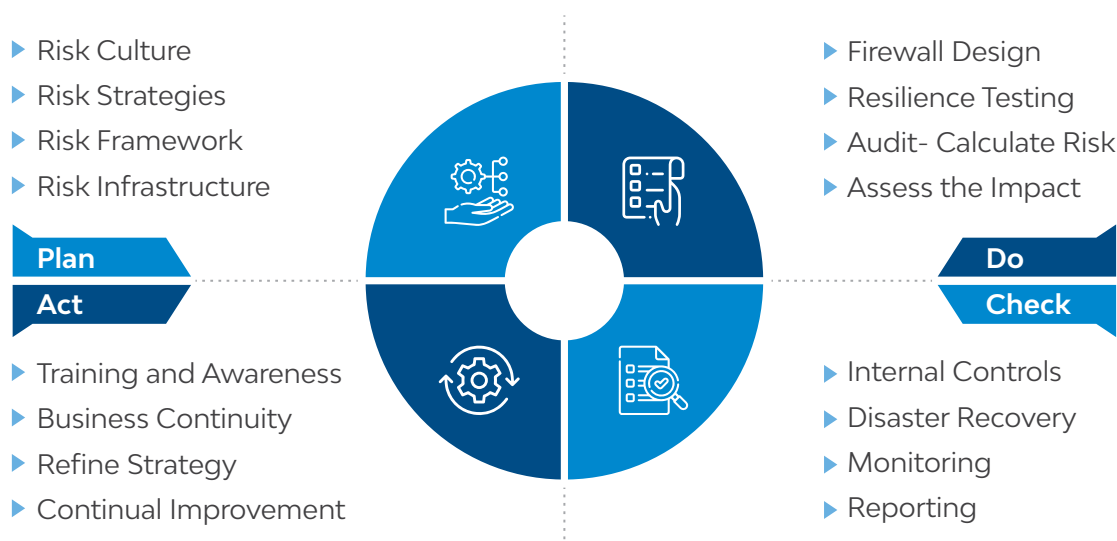
# Key Refurbishment Requirements



- Global regulations are intended to regulate risk management; however, they affect the entire financial enterprise. The senior management of a financial organization will have a key role in planning, executing, and meeting the regulatory compliance requirements.
- Essentially, the organization should determine its risk culture, business continuity strategy, recovery and response strategies, and communication policies and should determine its security controls of critical assets.
- The firm should have its streamlined reporting channel, incident warning/notification measures, data gathering, and major incident reporting mechanism.
- The organization should have resilient testing strategy and determine testing procedure, frequency, and tools to meet regulatory expectations.
- When needed, a firm should exchange cyber threat information within business units and must plan to raise awareness of cyber threats. The organization should plan for intelligence sharing with relevant communities.
- The concerned regulatory will monitor the compliance requirements of the Critical Cloud Service provider through its onsite/offshore inspections and audits. When these services are provided by third-party, risk management is a key area for which financial firms should stay more vigilant.

# Governance Framework- The Plan Do Check Act (PDCA) Cycle: Financial Organization Perspective

The key is how effectively financial organizations alter their governance landscape, which will determine rapid responses to changing statutory requirements.



● The financial services organization can use the PDCA cycle in order to determine the revised governance framework to meet the regulatory requirements. Based on the risk appetite, the organization shall design IT capacity, availability, security, and continuity. Robust measures shall be implemented through quality inspections and audits in order to check and identify security incidents.

● The resilience stress testing should prove the infrastructure quality in order to protect/secure against any type of cyber threat like Malware, Emotet, DoS, MITM, Phishing, SQL Injection, Password Attack, etc.

● In line with raising awareness of cyber threats, the organization shall arrange assessment-based frequent training programs for its business units and generate reports that can show the level of understanding.

● The C-suite executives will perform a key role in line with refining strategies and making decisions for capital optimization. They will assign relevant roles, monitor performance, and approve the organization's approach and governance framework.







# Next Step: Preparing for the New Reality

Well begun is half done!

There are already a few regulations in place in line with Cybersecurity and Data Privacy. The lawmakers are amending revised guidelines to make the existing regulations more robust and meaningful.

Additionally, the new regulations flow will continue to come in order to realign the business in the wake of new challenges.

Meanwhile, firms could start preparing and conducting events like Check, Conduct, and Calculate as depicted in the adjacent picture. This approach will help the firms in effective resource planning immediately.

| Activity   | Process   |
|--|---|
|  Check <span style="float: right;">▶</span>      | Determine whether organization or technology partner falls under which regulatory/regulation purview. |
|  Conduct <span style="float: right;">▶</span>   | Security Review, Determine the Gaps and Action Plan.  |
|  Calculate <span style="float: right;">▶</span> | The existing workload and book of work to comply .  |
|  Execute <span style="float: right;">▶</span>   | Risk and Governance Framework.  |
|  Develop <span style="float: right;">▶</span>   | Resilient Security Controls and Comprehensive Testing Plan.   |
|  Report <span style="float: right;">▶</span>    | Generate the evidence report based on data, remediate the security gaps and comply.                   |

**LTIMindtree** is here to help your enterprise to provide enhanced solutions to keep your business safe from data breaches.

LTIMindtree's Enterprise IT, Banking and Financial Services Consulting solution for the BFSI industry enable you to offer superior customer experiences and competitive business models, at the same time delivering extreme operational efficiency. Through LTIMindtree's advisory and implementation service offerings in the area of Cyber Defense Resiliency, our clients and end customers have realized many business benefits.

Our Consulting and Transformation services offering ensures a smooth transition, from the design and deployment stage to operations. In order to get the industry benchmark perspective of firms' readiness for Cybersecurity and Data Privacy, reach out to us at [www.ltimindtree.com](http://www.ltimindtree.com) to seek advice from our consulting expert.



# About the Author



## Shrikrishna Tirodkar

Associate Principal - Business Analysis, LTIMindtree.

Shrikrishna has over 17 years of experience in the field of BFSI and IT Industries. He is experienced in Capital Markets, Operational Risk, Life and Health Insurance, Linked Investment Service Provider Business, and Stock and Securities. At LTIMindtree, Shrikrishna is an Associate Principal in BFS Business Analysis/Consulting Group. He is deeply involved in consulting assignments focusing on Risk and Governance. His experience is related to various territories across the globe mainly the UK, US, South Africa, and India. He has a Masters in Management, PG+ in Business Intelligence, CBAP, and is a Certified Basel iii Professional of Basel iii Compliance Professional Association.

**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 — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit <https://www.ltimindtree.com/>