Grant Thornton

#GTBharat
SHAPING VIBRANT INDIA

Operational risk management and operational resilience

Building a resilient future

June 2024

Contents

Preface

On 24 April 2024, the Basel Committee on Banking Supervision (BCBS) published an updated version of its core principles for effective banking supervision. These core principles are among the most important global supervisory standards, establishing comprehensive requirements for supervisors and banks.

The core principles are a playbook that governments, regulators, and supervisors worldwide follow when adopting and assessing their supervisory rules and regulations. The revisions to the core principles explicitly focus on operational resilience, business model sustainability, and climate-related financial risks.

Recognising the global consensus on the relevance of these risks and a broad agreement on the need for action, on 30 April 2024, the Reserve Bank of India prepared and released a guidance note on operational risk management and operational resilience based on these principles of BCBS.

Recent years have been eventful and chaotic, with the pandemic, cyber incidents, technology failures, and natural disasters forcing supervisors to pay much closer attention to operational risk management and operational resilience.

Risks associated with operational failures stemming from processing errors, internal and external fraud, legal claims, and business disruptions have existed in this industry since its inception. However, the operational environment for many financial institutions has evolved significantly in recent years owing to the globalisation of financial services, the introduction of new and highly complex products, growth in e-banking transactions and the adoption of automation.
The COVID-19 pandemic has exaggerated these operational risks and increased economic and business uncertainty.

Technology and relationships with third parties have supported the continued delivery of products and services to customers and promoted banks' ability to continue operations during the pandemic; however, these have opened doors to significant, varied risks.

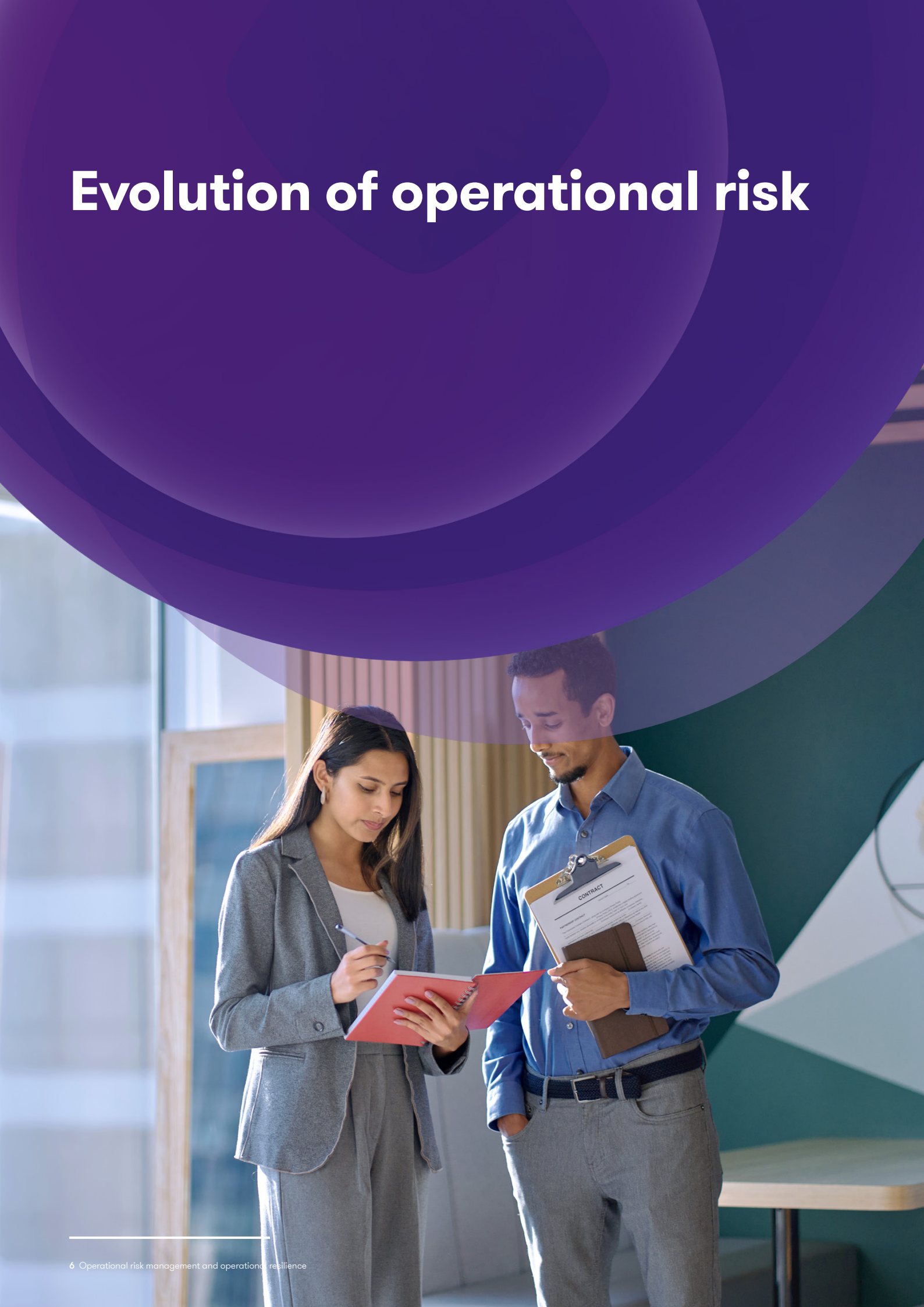
While operational risk is inherent in all banking/financial products, services, activities, processes, and systems, the financial sector's growing reliance on third-party providers (including technology service providers) intensified during the COVID-19 pandemic, with greater reliance on virtual working arrangements. This highlights the increasing importance of operational risk management and operational resilience.

Operational risk management allows financial institutions to identify, assess, and mitigate operational risks, while operational resilience provides them with the ability to deliver critical functions in the event of any disruption. Although operational risk management and operational resilience address different goals, they are closely interconnected. An effective operational risk management system and robust operational resilience must work together to reduce the frequency and impact of operational risk events.

While the market had its understanding of operational risk and operational resilience, a regulatory direction always helps provide greater clarity and facilitate standardisation, both of which are important for effectively managing financial stability risk.

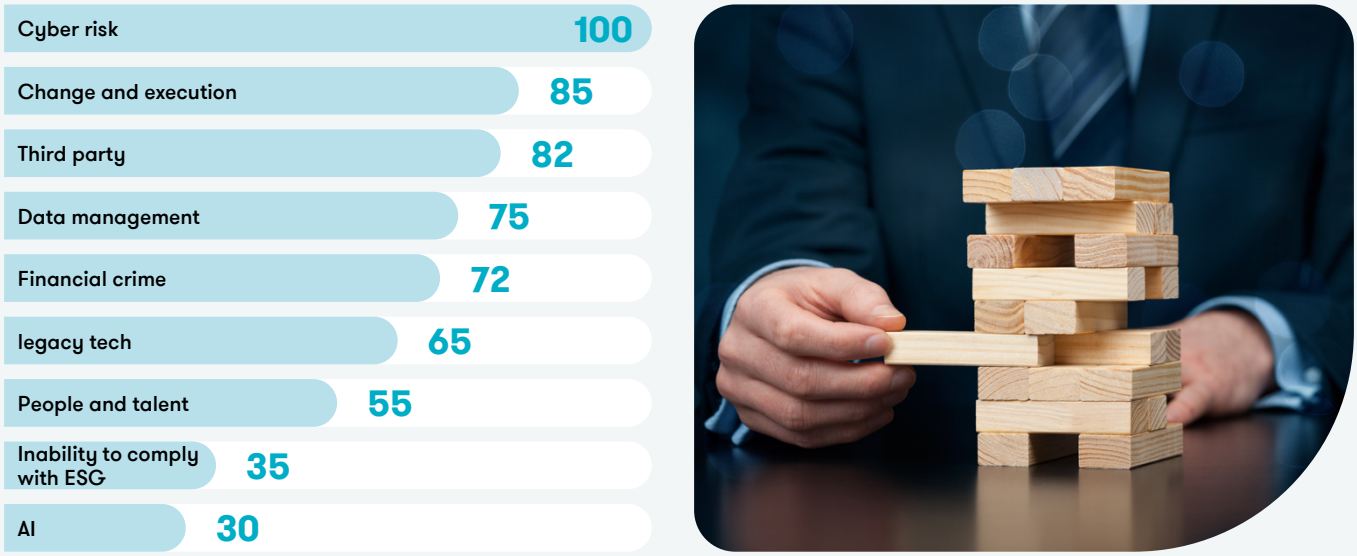
Vivek Iyer
Partner, FS Risk
Grant Thornton Bharat

Evolution of operational risk



Operational risk, as compared to others, has garnered significant attention and concerns in the last two decades. In the early 2000s, Basel introduced a series of papers introducing operational risk and requiring its management. Initially, banks and financial institutions took measures like loss event reporting, risk control self-assessments, and developing risk capital models.

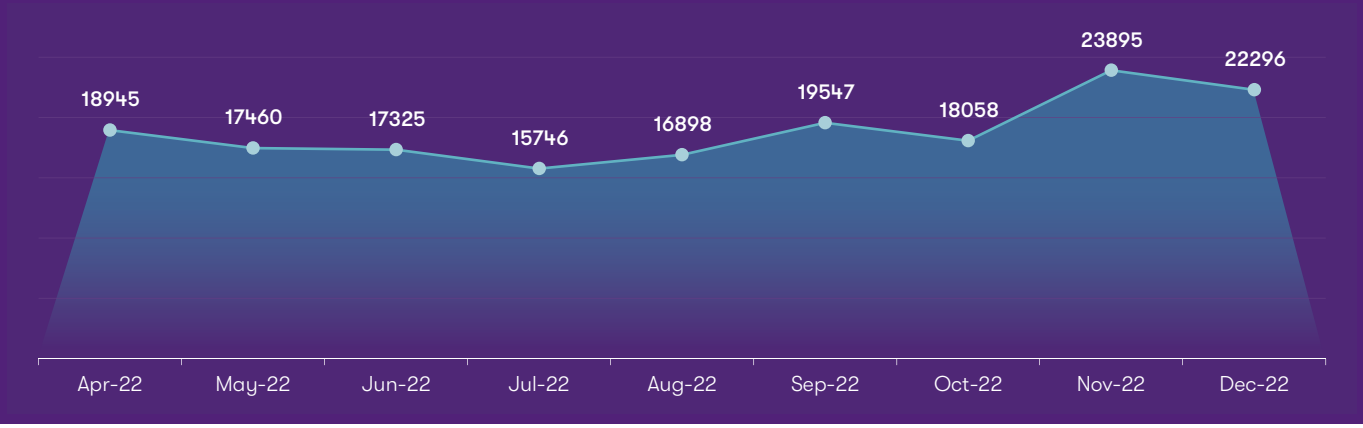
However, the operational risk landscape transformed dramatically, marked by operational failures from events like processing errors, internal and external fraud, legal claWims, and business disruptions. The financial crisis further exposed numerous malpractices, including London Inter-bank Offered Rate (LIBOR) manipulation, economic crimes, foreign exchange misconduct, misclassification, and issues with the valuation and operation of investment portfolios. These issues led to significant regulatory fines and enforcement actions.



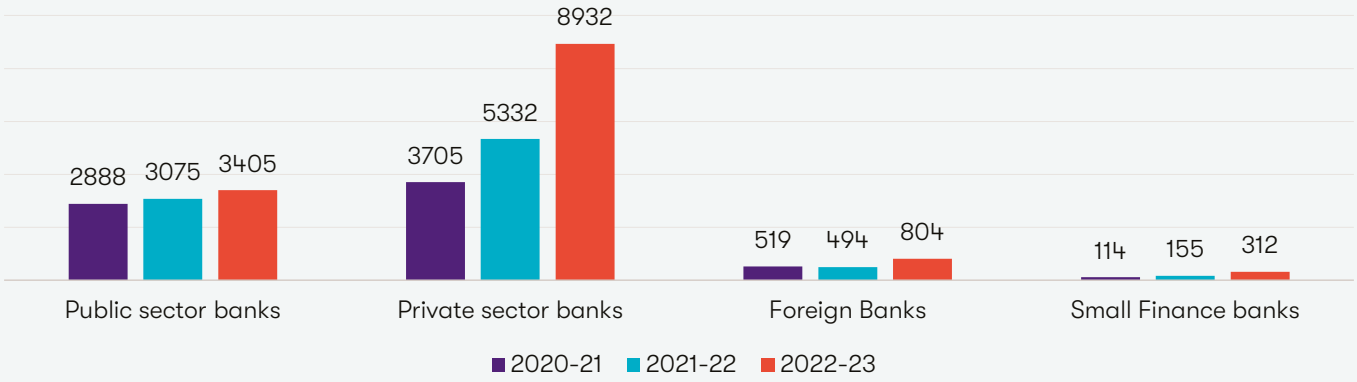
This highlighted the need to reexamine the existing control environment. The financial institutions have responded by making significant changes in operational risk capabilities, implementing new risk identification and risk assessment processes, and creating extensive controls and control-testing processes.

While there has been some progress in managing operational risk, losses from operational risk have remained elevated. As seen by the following indicators of operational risk, customer complaints have been steadily increasing since 2022.

Complaints received



Increasing trend of fraud in the banking industry



Need for increased regulatory focus

Operational risk identification and measurement are still in an evolutionary stage compared to the maturity that market and credit risk measurements have achieved.

The regulator widely recognises the need for operational risk management, and various circulars and guidance notes outlining guidelines for it have been issued thus far.

- Risk Management Systems in Banks, 1999
- Draft Guidance Note on Management of Operational Risk, 2005
- Operational Risk Management - Business Continuity Planning, 2005
- Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, 2006
- Master Direction on Minimum Capital Requirements for Operational Risk, 2023
- Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023
- Guidance Note on Operational Risk Management and Operational Resilience, 2023
- Master Direction on Outsourcing of Information Technology Services, 2023

Despite the efforts of regulators and financial institutions, managing operational risk remains a significant challenge. This difficulty arises from the diverse and dynamic nature of operational risk, including cyber risk, financial crime, and compliance issues.

In the first circular on risk management in banks in 1990, operational risk was defined as any risk apart from credit, market, and liquidity risks, highlighting its extensive interconnection across the entire organisation. Often, operational risks are only identified after they have significantly impacted the organisation. Due to its pervasive nature, identifying, measuring, and managing operational risk remains daunting.

The Indian apex bank is aware of this and is actively addressing it, as is evident from their recent actions, including penalties and regulatory actions.

Recent penalties imposed by the regulator

INR 12.19 crore

A top private indian bank

Non-compliance with the RBI directions on 'frauds classification and reporting by commercial banks and select FIs

A large private bank

Non-compliance with RBI directions on outsourcing

INR 1.40 crore

INR 84.6 lakh

A top public sector bank

Non-compliance with the RBI's directions related to 'interest rate on deposits', 'customer service in banks', 'interest rate on advances.'

A large Indian public sector bank

Non-compliance with the RBI directions on 'frauds classification and reporting

INR 84.6 lakh

INR 49.7 lakh

One of the largest housing finance companies

Breach of norms of the Fair Practices Code

A new approach

The evolution of operational risk management is moving towards a proactive framework, requiring the industry to move beyond a rear-view mirror approach. This involves evaluating the uniqueness of business processes and their interdependencies, continuously learning and adapting from incidents and failures, and generally increasing the organisation's preparedness and resilience.

The guidance note has been drafted based on the Basel Committee on Banking Supervision (BCBS) principles issued in March 2021, aligning the approach regulated entities should take to build operational resilience.

The revised note replaces the precursor Guidance Note from 14 October 2005, laid down primarily for the scheduled commercial banks. It now extends its purview to many financial institutions, such as co-operative banks, all-India financial Institutions, and non-banking financial institutions.

The regulator has now adopted an approach that defines 17 principles covering the key elements of operational risk management and operational resilience across three pillars – 'Prepare and protect', 'Build Resilience' and 'Learn and Adapt'.

The note explains the 'Three lines of defence model', wherein a business unit forms the first line of defence, the organisational and operational risk management function (including the compliance function) forms the second line of defence, and the Internal Audit function forms the third line.

Prepare & protect

- Governance and risk culture
- Responsibilities of Board of Directors and senior management
- Risk management environment - Identification and assessment
- Change management
- Monitoring and reporting
- Control and mitigation

Build resilience

- Mapping of interconnections and interdependencies
- Third-party dependency management
- Business continuity planning and testing
- Incident management
- Information and Communication Technology (ICT) including cyber security

Learn & adapt

- Disclosure and reporting
- Lessons learned exercise and adapting
- Continuous improvement through feedback systems

Key changes

Enhanced coverage

The Indian economy is one of the fastest growing in the world. Despite the global unrest, it is expected to grow 6.5% in FY 2024. The demand for credit to support this economic growth has sharply increased.

As of 31 March 20241, there are 9327 NBFCs registered with RBI, including housing finance companies. With its all-pervasive nature, the operational risk inherently applies to all financial institutions.

However, structured guidance was only available for scheduled commercial banks. The growth of these financial institutions—cooperative banks and all-India financial institutions—and the impact of their operations warranted focused operational risk management guidance.

This guidance note has been extended to cooperative banks, all-India financial institutions, and non-banking financial companies (NBFCs). The extension of applicability may be a proactive approach by regulators to strengthen the financial system's resilience and safeguard against potential disruptions or crises.

Increased focus on operational resilience

Businesses today encounter a broader range of disruptions than ever before, including cyberattacks, natural disasters, pandemics, economic downturns, and political instability. These disruptions can severely affect an organisation's ability to function. Businesses becoming increasingly reliant on technology makes them more vulnerable to outages and cyberattacks.

While the term itself might be recent, the concept behind operational resilience has long existed. Traditionally, it was addressed through practices like disaster recovery planning. However, the growing number and variety of threats have led to a more comprehensive approach. Initially, the focus was on recovering from physical disasters like fires or floods. As technology dependence grew, the need to plan for cyberattacks became a significant concern.

Regulations like the Digital Operational Resilience Act (DORA) emphasise the importance of operational resilience in critical sectors like finance. By building operational resilience, businesses can be better prepared to handle these disruptions and minimise their impact.

The nature of operational risk is such that its impact will not be felt until it has crystalised as fraud, theft, financial penalties, regulatory investigations, etc. While credit, market, and liquidity risks can be preempted from various metrics, it is inherently challenging to identify operational risk events until they cause a more significant disruption.

The regulator has increased their focus on operational resilience in tandem with operational risk management instead of relying on operational risk management alone.

Reinforcing the 3LoD approach

The RBI's increased focus on the 'Three Lines of Defence' (3LoD) model is driven by recognising the critical importance of robust operational risk management within Regulated Entities (REs), particularly amid heightened incidents of operational losses and fraud globally.

Historically, traditional risk management frameworks often overlooked operational risks, leading to vulnerabilities within financial institutions. The 3LoD model ensures a structured approach to operational risk management, delineating clear roles and responsibilities among business units, oversight functions, and audits, thus promoting accountability, transparency, and effective risk mitigation strategies within REs.

This framework aligns with global standards set by the Basel Committee on Banking Supervision (BCBS), ensuring a globally consistent approach to operational risk management in banking. It emphasises clear roles and responsibilities, adequate resources, and effective communication between the lines.

The 3LoD framework promotes effective collaboration between different functions within a bank, creating a robust shield against operational risks. This approach safeguards individual REs by promoting a layered approach to risk mitigation and contributes to the stability of the entire financial system.

Heightened focus on change management

The financial sector has grown increasingly complex with the emergence of new products, markets, technologies, and regulations. These changes can introduce new operational risks, making managing such risks complex without a structured approach.

Traditional risk management practices may no longer suffice to address the evolving risks associated with constant change. Past operational failures in the financial sector, often linked to poorly managed changes, have underscored the need for a more robust framework. As a result, the RBI has placed greater emphasis on operational resilience.

Highlighting the interconnections and interdependencies

In the last decade, we have faced unexpected public health catastrophes, cybersecurity threats, significant protests, terrorism, and climate-related events such as severe floods and fires. These experiences demonstrate that disruptions to daily functions are inevitable for financial institutions. Even before the pandemic, the Basel Committee had anticipated that considerable operational disruptions would test the resilience of financial systems.

Therefore, it is necessary to identify critical operations and map the internal and external interconnections and interdependencies to deliver critical operations consistent with its approach to operational resilience.

Each of its functions—people, information, processes, facilities, and their interconnections and interdependencies—should be mapped to facilitate the critical operations of the bank.

The regulator imposing curbs on a leading private sector bank in India over inefficiencies in its IT management framework, which led to a 10-hour disruption, highlights the increased regulatory focus on information and communication technology.

Previously, the regulator did not require financial institutions to identify and map internal and external interconnections and interdependencies, incident management, and information and communication technology. However, with the BCBS including these aspects as principles of operational risk management, the regulator has increased its focus on these areas.

All regulated entities must now map such interdependencies at a granular level to identify vulnerabilities and support testing their ability to deliver critical operations through disruptions.

Re-aligning third-party relationships

Financial institutions have constantly engaged third parties to provide services and deliver functions. Engaging with third parties exposes financial institutions to a wide range of risks, such as cyberattacks, potential regulatory fraud, non-compliance, business disruptions, penalties, and fines due to these risks. Through multiple regulatory circulars and guidelines, the RBI has consistently maintained that financial institutions must address third-party risks holistically.

Given the potential impact of their disruption on financial institutions' critical operations and financial stability, there has been an increased regulatory emphasis on critical third-party services.

RBI has issued various circulars for guidelines on managing risk in outsourcing financial services owing to the increase in outsourcing to reduce costs and avail specialist expertise.

Outsourcing guidelines

- Guidelines for Managing Risk in Outsourcing of Financial Services by Co-operative Banks, 2021
- Master Direction - Non-Banking Financial Company - Housing Finance Company (Reserve Bank) Directions, 2021
- Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs, 2017
- Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks, 2015
- Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks, 2008
- Outsourcing of Financial Services - Responsibilities of regulated entities employing Recovery Agents, 2022

These circulars provide scattered guidance on various aspects of outsourcing risks. They cover considerations for outsourcing risks, permissible functions for outsourcing, and establishing an outsourcing framework that delineates the roles and responsibilities of senior management and the board. Additionally, they mandate periodic monitoring of outsourced activities and emphasise the importance of due diligence by service providers or vendors.

Through this guidance note, the RBI has created a holistic document encompassing all the previously issued guidelines focused on third-party relationship management, a broader concept than outsourcing.

There is a need to holistically examine financial institutions' third-party risk management, considering changing industry practices and recent regulatory and supervisory approaches to operational resilience.

Augmenting lessons learned and continuous feedback mechanism

In recent times, we have witnessed various categories and severity of operational risk loss events, such as

- An American multinational finance company had to pay USD 350 million for incomplete trading data fed to the market surveillance system
- An American multinational investment bank and financial services company had to pay USD 249.4 million for leaking confidential information on block trades
- An American multinational financial service had to settle USD 81.7 million over wrongful car repossession claims
- On the domestic front – one of the leading private sector banks is prohibited from onboarding new customers through online and mobile banking channels owing to the bank's weaknesses in IT infrastructure
- The regulator imposed monetary penalty on five cooperative banks citing non-compliance with the operational instructions issued by them

From the above, it is clear that banks, NBFCs, and other financial institutions have gained significant insights into identifying, mitigating, and addressing gaps in their operational risk management frameworks. A recurring theme is how these institutions have pinpointed vulnerabilities in their systems and processes that led to failures or disruptions in delivering critical business operations. In the dynamic and ever-evolving environment in which financial institutions operate, promptly addressing the root cause of these issues is of prime importance.

With this guidance note, the regulator has emphasised continuous learning about the disruptions caused and ensuring that the feedback is incorporated into the operational risk management framework to be prepared in line with the increased focus on operational resilience.

Although indicative, the principles discussed in the guidance note are generally accepted and followed by banks but have significantly impacted the other entities covered in the gamut of this guidance note. The impact on the regulated entities, stemming from the guidance note are as follows:

Impact assessment

Governance and risk culture

Principle 1

The Board of Directors should take the lead in establishing a strong risk management culture, implemented by senior management. The Board of Directors and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behavior, and ensure that staff receives appropriate risk management and ethics training.

Board and senior management should be at the forefront of establishing a strong risk management culture. To implement or enhance this culture, the REs need to focus on the following action points:

- Establish a code of conduct or ethics policy applicable to staff and Board members, setting clear expectations for integrity, ethical values, acceptable business practices, and the prohibition of conflict of interest
- Establish regular reviews, approvals by the BOD, and attestation by the employees under the oversight of a Senior/Board-Level committee
- Set clear expectations, define accountabilities for staff, and build communication channels across the organisation regarding the staff's role in risk management, responsibilities, and authority to act
- Align compensation policies with the RE's risk appetite, tolerance, and overall risk management framework, reducing inappropriate incentivisation risk
- Develop a focused training framework to cover operational risk training across all organisational levels. The framework should encompass coverage and content resonating with applicability, staff seniority, roles, responsibilities, training plan, defined frequency of training, and monitoring mechanism

Principle 2

The REs should develop, implement, and maintain an ORMF that is fully integrated into the RE's overall risk management processes. The ORMF adopted by an individual RE will depend on a range of factors, including its nature, size, complexity, and risk profile. Further, REs should utilise their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events to minimise their impact on delivering critical operations through disruption.

REs over time have adopted operational risk and internal control mechanisms in some form. To standardise and ensure an optimal level of coverage, the REs should consider the following action points:

- Leverage and build on existing governance structures to establish an effective operational resilience approach
- Boards and senior management should establish a mechanism for understanding and comprehending the inherent and potential risks associated with new business initiatives, products, services, activities, processes, and systems
- Components of ORMF should be integrated into the RE's risk management processes through the first, second, and third lines of defense: Comprehensive documentation and referencing within board-approved policies, usage of defined tools for risk and control identification and assessment, defined operational risk appetite, establishing a common risk taxonomy, and regular engagement across business units
- While senior management should be responsible for managing operational risk, a channel for regular reporting of on-the-ground information to the Board should be established to ensure oversight and accountability

Responsibilities of Board of Directors and senior management

Principle 3

The Board of Directors should approve and periodically review the ORMF and operational resilience approach and ensure that senior management implements the policies, processes, and systems of these approaches effectively at all decision levels.

Following are the responsibilities and corresponding action points to be driven through the Board of Directors of the REs:

- Establish a comprehensive risk management culture and establish robust oversight of the operational risk management processes
- Define clear directives for senior management on implementing and adhering to ORMF principles, approve corresponding policies, and regularly review and evaluate their effectiveness through an established board reporting mechanism
- Enable strengthening of independent review of the ORMF facilitated by the third line of defence
- Define clear management responsibility and accountability for implementing a strong control environment.
- Provide directives on setting up an internal control mechanism that optimally covers the business and support functions, defines roles between the first and second line of defence, and includes a periodic control testing mechanism.
- Active participation during the implementation and dissemination of the RE's operational resilience approach.
- Drive the review and approval mechanism of the operational resilience approach at regular intervals, encompassing risk appetite and tolerance for disruption to critical operations and management of exceptions thereof

Principle 4

The Board of Directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk the RE is willing to assume. The Board of Directors should also review and approve the criteria for identification and classification as critical operations as well as of impact tolerances for each critical operation enhance RE's operational resilience.

To adopt this principle, the RE should consider the following action points:

- Develop and adopt a risk appetite and tolerance statement under the authority of the Board of Directors
- The risk appetite statement should document the RE's approach to risk management, its risk universe, the nature of risks and the corresponding level of risk the RE is willing to assume and tolerance limits
- Define critical operations based on customer risk, RE viability, safety, soundness, and financial stability. The criteria should be reviewed annually or when business changes materialise
- Define and quantify impact tolerances to derive the maximum acceptable disruption level, which should be tested against plausible scenarios. The Board should review and approve impact tolerances for each critical operation annually or as disruptions occur

Principle 5

Senior management should develop for approval by the Board of Directors a clear, effective, and robust governance structure with well-defined, transparent, and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes, and systems for managing operational risk in all the RE's material products, activities, processes, and systems consistent with its risk appetite and tolerance statement.

This principle talks about implementing a documented operational risk management framework. The following action points, driven by the senior management, become pivotal to the operationalisation.

- Split the ORMF into adaptable and functional policies and procedures. The corresponding documentation should clearly identify and call out the authority, responsibility, and reporting relationships
- Implement the documented policies and procedures to demonstrate the availability of resources, involvement from all relevant stakeholders and flow of communication to and from the Board
- Establish strong challenge mechanisms and effective issue-resolution processes. This includes issue tracking, reporting, exception and escalation management, issue closure and validation, impact analysis, root cause analysis and issue repository
- Establish effective communication channels and coordination between operational risk staff and other departments, such as credit risk, market risk, and the procurement team managing external services, to avoid gaps and overlaps
- Ensure capability —and experience-based hiring across managerial and support staff, as demonstrated by the availability of appropriate job cards and KRAs., etc.
- Design of the operational risk governance structure should consider:
  - Setting up of operational risk committee either separately or taken up by the Board's risk management committee depending on the size and scale of the entity
  - The committee should comprise members with expertise in business activities, financial activities, legal, technological and regulatory matters, and risk management
  - Frequency of committee meetings, record of the meeting, key discussions and decisions should be documented

Risk management environment - Identification and assessment

Principle 6

Senior management should ensure that the RE's change management process is comprehensive, appropriately resourced, and adequately articulated between the relevant lines of defence.

An ideal change management mechanism should assess the evolution of associated risks from inception to termination. To comply with this principle, the REs should consider the following action points:

- Develop specific policies and procedures documented to handle the change management process. These should be policies and procedures documented to handle the change management process and should be subject to independent and regular review and update.
- The documentation should call out the responsibilities across the three lines of defence – first line being the owner of the change (new product/process, etc.) and hence performing the risk and control assessment, second line bringing in the challenge mechanism, third line bringing in the independent review
- The risk assessment changing from any change management exercise should document the following:
  - Inherent Risks related to the new product/process/system
  - Changes to REs risk profile or risk appetite, if any, stemming from the said change
  - Changes to risk thresholds if any
  - Functional controls in place, control gaps, if any, and corresponding residual risk
- A review and approval mechanism are in place through a senior committee and all upstream and downstream stakeholders. The review and approval mechanism are in place in the form of a senior committee, along with all upstream and downstream stakeholders, from an impact perspective
- Develop a formal note documenting the change envisioned for the investment made and noting investments made in human resources and technology infrastructure before changes are introduced
- REs should implement a monitoring mechanism during and after the implementation to identify any material differences to the expected operational risk profile and manage any unexpected risks
- REs should maintain a central record of products and services to facilitate change monitoring

Change management

Principle 7

Senior management should ensure the comprehensive identification and assessment of the operational risk inherent in all material products, activities, processes, and systems to ensure the inherent risks and incentives are well understood. Both internal and external threats and potential failures in people, processes and systems should be assessed promptly and on an ongoing basis. Assessment of vulnerabilities in critical operations should be done manner proactively and promptly. All the resulting risks should be managed in accordance with the operational resilience approach.

Risk identification and assessment are the first steppingstones to an effective operational risk management system in effect. These steps, in turn, help senior management comprehend its risk profile, deploy risk management strategies, and allocate resources effectively. From that point of view, the RE has the following action points to consider:

- Assess and employ relevant risk identification and assessment tools in alignment with the ORMF framework and policies defined
- The tools should highlight process and activity-level risks, corresponding controls and their efficacy, operational losses, near misses, scenarios, treatment, etc.
- The department running these exercises should ensure the accuracy of the input data and should be supported by action tracking and remediation plans wherever applicable
- Conduct regular operational risk assessments as defined in the ORMF, specifically after incidents, to incorporate lessons learned and address new threats and vulnerabilities affecting critical operations

Monitoring and reporting

Principle 8

Senior management should implement a process to regularly monitor operational risk profiles and material operational exposures. Appropriate reporting mechanisms should be in place at the Board of Directors, senior management, and business unit levels to support proactive management of operational risk.

This principle states that the RE should have a strong reporting mechanism that facilitates the senior management and the Board in timely action and course correction. This can be facilitated through the following action points:

- The first line of defence should define the metrics to be reported. This should include residual risks, control gaps, ineffective processes, risk events, operational losses and non-compliance
- The reports should be available in both standard and stressed market conditions
- Frequency of the reports should be defined
- Ownership of the reports should be defined and documented along with the recipients of the reports, who should roll up to senior management and the board.
- The results of monitoring activities should be included in regular management and Board reports, as should assessments of the ORMF performed by the internal/external audit or risk management functions
- Review of data capture and risk reporting processes should be performed at regular intervals

Control and mitigation

Principle 9

REs should have a strong control environment that utilises policies, processes, and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

This principle addresses the need for an RE to have a robust internal controls mechanism documented in a policy or manual to provide reasonable assurance that it will have efficient and effective operations, safeguard its assets, produce reliable financial reports, and comply with applicable laws and regulations.

- Implement a system (or at least a well-defined mechanism depending on the size and scale of the entity) to ensure internal and external compliance with policies, procedures and regulatory requirements
- Ensure that segregation of duties is established appropriately to prevent conflicts of interest and concealment of losses
- Integrate technology risks into the overall risk management framework and ensure they are adequately identified, measured, monitored, and managed
- Assess and mitigate risks associated with third-party dependencies, including concentration of risk, complexity, and downstream dependencies
- Evaluate the option of risk transfer through insurance or other means, but ensure it complements internal control mechanisms rather than replacing them entirely. In such a case, RE must review insurance needs annually
- Implement a monitoring mechanism during and after the implementation to identify any material differences to the expected operational risk profile and manage any unexpected risk
- Maintain a central record of products and services to facilitate change monitoring

Mapping of interconnections and interdependencies

Principle 10

Once an RE has identified its critical operations, it should map the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.

As prescribed by the guidance note, identifying critical processes is a precursor to this activity. This stem from the notion that 'operational resilience is the acceptance that disruptions will occur, and that REs need to be prepared to respond accordingly'. Operational resilience rests on multiple factors, with critical operations at the centre.

- Post identifying critical operations, map the internal and external interconnections and dependencies necessary for their delivery, aligned with their operational resilience approach
- Identify and document people, technology, processes, data and information, facilities, and their interconnections and dependencies required for critical operations delivery, including those involving third parties or intragroup arrangements wherever applicable
- Initiate this exercise for critical functions but, in course of time, extend it to all the functions to ensure holistic coverage
- Mapping of interdependencies should be detailed enough for REs to identify vulnerabilities and support testing of their ability to deliver critical operations during disruption, considering their risk appetite
- If part of a group, account for additional risks persistent in the group that may affect their ability to handle severe disruptions to operations

Third -party dependency management

Principle 11

REs should manage their dependencies on relationships, including those of, but not limited to, third parties (which include intragroup entities), for the delivery of critical operations.

For effective management of dependencies on third parties or other relationships, REs should consider the following action points:

- Perform risk assessments and due diligence to ensure equivalent levels of operational resilience aligned with their ORMF and third-party risk management policy
- Set up an ongoing review of third parties to ensure sustained dependency management
- Document the periodicity of such reviews and the coverage in the form of a Board-approved vendor risk management/outsourcing policy
- The policies and procedures laid down should cover the following:
  - Activity for determining the need for third-party arrangements
  - due diligence processes
  - structuring of arrangements
  - risk management
  - control environment establishment
  - contingency planning
  - comprehensive contracts or service-level agreements (defining data confidentiality, periodic review, allocation of responsibility and handoff, subcontracting)
- Develop business continuity procedures and exit strategies to maintain operational resilience in case of third-party failures or disruptions, assessing substitutability of third parties and considering alternatives like bringing services in-house

Business continuity planning and testing

Principle 12

REs should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption. Business continuity plans should be linked to the RE's ORMF. REs should conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption

Effective governance of business continuity plans should be facilitated through the following:

- Regular review and approval by the Board, involvement of senior management and business units, commitment from the first and second lines of defence, and regular review by the third line of defence
- Prepare forward-looking business continuity plans grounded on scenario analyses and impact assessments, covering critical operations, dependencies, and recovery procedures
- Business continuity plans should include key elements such as
  - Crisis communication plan
  - Stakeholder information
  - Business impact analysis
  - Testing programs
  - Training program
  - Critical operations and interdependencies, including those with third parties and intragroup entities
  - Details of acceptable downtime and RTO
- Plans should provide detailed guidance for implementing the RE's disaster recovery framework, defining roles, responsibilities, decision-making processes, and triggers for invoking the business continuity plan

Incident management

Principle 13

REs should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the RE's risk appetite and tolerance for disruption. REs should continuously improve their incident response and recovery plans by incorporating lessons from previous incidents.

In alignment with the business continuity planning, the RE should focus on the response and recovery piece to ensure robust operations. Following are the action points suggested for the REs:

- Develop and maintain, on an ongoing basis, an inventory of incident response and recovery, internal and third-party resources
- Document incident management to cover the entire incident life cycle, including
  - severity classification
  - relevant stakeholder listing
  - response and recovery procedures
  - alignment to business continuity and disaster recovery plans
  - communication plans for internal and external stakeholders
  - lessons learnt and previously accepted approaches
- Document a communication plan to cover escalation routes and details on communicating with decision-makers, operational staff, third parties, customers, stakeholders, and regulators
- Regularly review incident response and recovery procedures, tested and updated by REs to ensure effectiveness and identify and address root causes to prevent recurrence

Information and Communication Technology (ICT) including cyber security

Principle 14

REs should implement a robust Information and Communication Technology (ICT) risk management programme in alignment with their ORMF and ensure a resilient ICT, including cyber security that is subject to protection, detection, response, and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant, timely information for risk management and decision-making processes to fully support and facilitate the delivery of the RE's critical operations.

Robust ICT risk management for the REs can be facilitated though the following:

- Document ICT policy, including governance requirements, risk ownership, security measures, incident response, and business continuity plans
- Develop an oversight mechanism for the effectiveness of ICT risk management, aligning business, risk management, and ICT strategies with the RE's risk appetite and tolerance
- Establish regular reviews for ICT risk management, considering industry standards and evolving threats. These reviews should be tested to identify gaps and actionable intelligence should be used to enhance situational awareness
- Develop ICT readiness approaches for stressed scenarios from disruptive external events, with commensurate risk mitigation strategies, management of privileged users, and regular updates to management
- Prioritise cybersecurity efforts based on ICT risk assessment and the significance of critical information assets while complying with legal and regulatory requirements for data protection and confidentiality

Disclosure and reporting

Principle 15

REs should manage their dependencies on relationships, including those of, but not limited to, third parties (which include intragroup entities), for the delivery of critical operations.

From a perspective of adequate disclosures, the REs should

- Provide public clear disclosures that allow stakeholders to assess their approach and exposure to operational risk
- The extent and type of disclosure should be appropriate for the size, risk profile, complexity of operations, and evolving industry standards of the RE
- Disclosure of the Operational Risk Management Framework (ORMF) should call out RE's effectiveness in identifying, assessing, monitoring, and controlling/mitigating operational risk
- It should not create additional operational risk through the excess disclosure
- Develop a formal disclosure policy subject to regular and independent review and approval by senior management and the Board of Directors
- Outline the approach for determining disclosures, controls over the disclosure process, and mechanisms for assessing their appropriateness.

Lessons learnt exercise and adapting

Principle 16

A lesson-learned exercise should be conducted after a disruption to critical business service to enhance an RE's ability to adapt and respond to future operational events

Lessons learnt exercise enables the REs to bring the knowledge and experience from the past to build a forward-looking mitigation mechanism. The REs should consider the following action points have a suitable "lessons learnt" exercise in place:

- Perform root cause analysis, particularly focusing on disruptions to critical services
- Document a repository of information from past incident management and disaster recovery processes, corresponding key decisions taken and adapted recovery processes
- Analyse patterns if any, from previous incidents and disruptions.
- Define criteria or questions for the exercise to identify deficiencies causing service interruptions
- Define remediation measures against the causes identified, and map them against corresponding departments to establish accountability
- Develop an action plan for improving risk management practices, strengthening controls, and enhancing operational resilience after implementing the recommendations
- Establish a mechanism for the presentation of the assessment exercise to the Board
- Conduct periodic reviews and updates to ensure that lessons learned are integrated into ongoing risk management practices and processes

Continuous improvement through feedback systems

Principle 17

An RE should promote an effective culture of learning and continuous improvement as operational resilience evolves through effective feedback systems.

To implement a culture of learning and continuous improvement within an RE, especially in the context of operational resilience, the following action points can be considered:

- Promote a culture of learning and continuous improvement through a top-down approach
- Demonstrate leadership commitment to the cause
- Develop and implement a robust feedback system to ensure the smooth functioning of the feedback loop.
- Ensure the feedback system covers the identification and assessment of the type, and severity of potential operational risks that an RE could face
- Continuously review feedback mechanisms to ensure they remain effective and responsive to evolving needs and challenges
- Periodically assess the impact of feedback on operational resilience outputs to update and make necessary adjustments

Acknowledgements

Contributors

Vivek Iyer
Partner, FS Risk
E: vivek.iyer@in.gt.com

Vidhi Sanghvi
Manager, FS Risk
E: vidhi.sanghvi@in.gt.com

Vernon Dcosta
Partner, FS Risk
E: vernon.dcosta@in.gt.com

Shweta Patange
Manager, FS Risk
E: shweta.patange@in.gt.com

Rajeev Khare
Director, FS Risk
E: rajeev.khare@in.gt.com

Mamta Vora
Manager, FS Risk
E: mamta.vora@in.gt.com

Dharmesh Jadav
Director, FS Risk
E: dharmesh.jadav@in.gt.com

Editorial review
Shabana Hussain

Design
Vikas Kushwaha

For media enquiries, write to
media@in.gt.com

Great Place To Work® Certified DEC 2023 – DEC 2024 INDIA ™

Best Workplaces™ in Professional Services
Great Place To Work® INDIA 2023

We are
Shaping Vibrant Bharat

A member of Grant Thornton International Ltd., Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more **#VibrantBharat.**

Our offices in India

- Ahmedabad
- Bengaluru
- Chandigarh
- Chennai
- Dehradun
- Delhi
- Goa
- Gurgaon
- Hyderabad
- Kochi
- Kolkata
- Mumbai
- Noida
- Pune

Scan QR code to see our office addresses
www.grantthornton.in

Connect with us on

@Grant-Thornton-Bharat-LLP
@GrantThorntonBharat
@GrantThornton_Bharat
@GrantThorntonIN
@GrantThorntonBharatLLP
GTBharat@in.gt.com

7075 | SH | VK