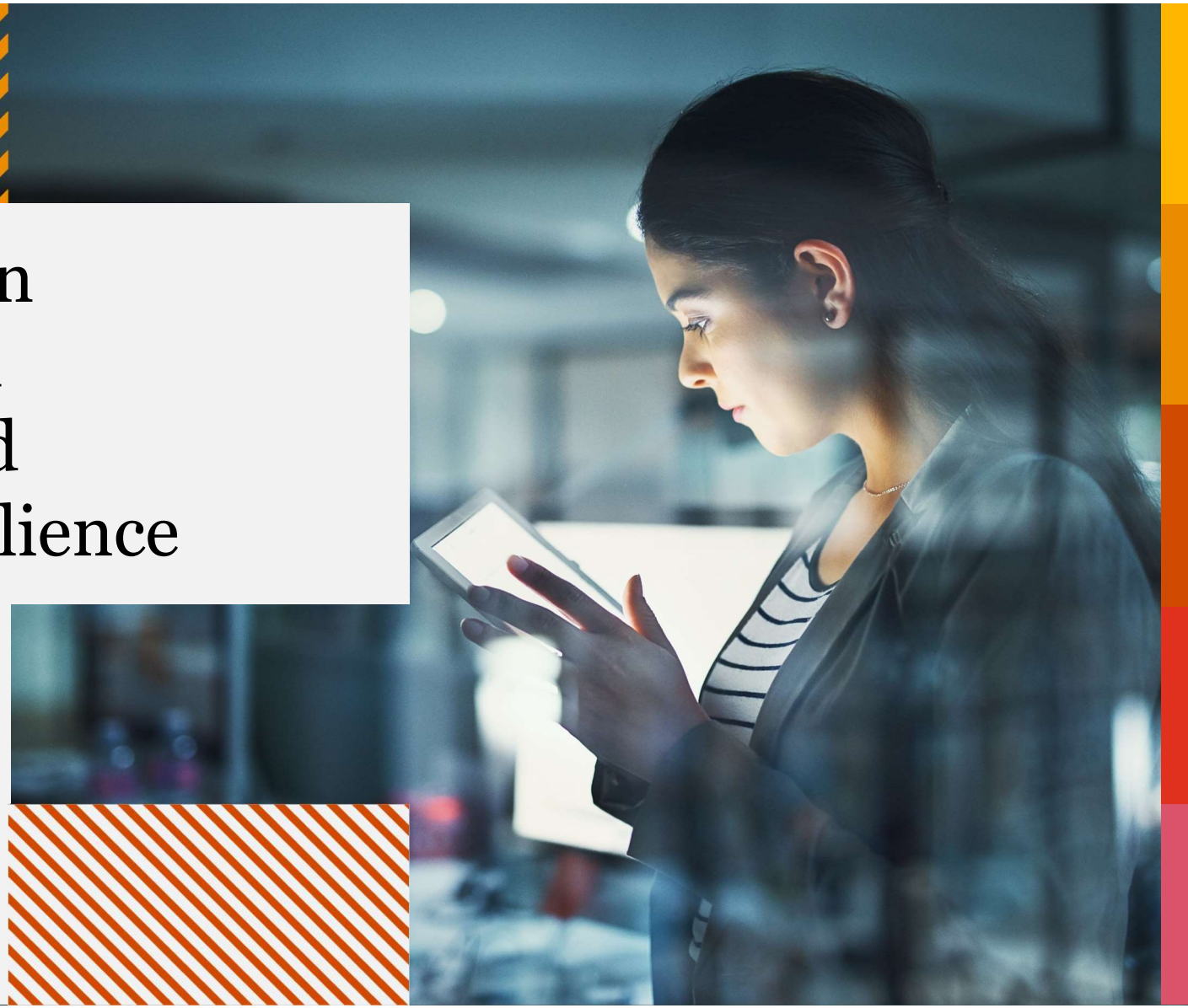
Guidance Note on Operational Risk Management and Operational Resilience



A PwC perspective

June 2024

pwc

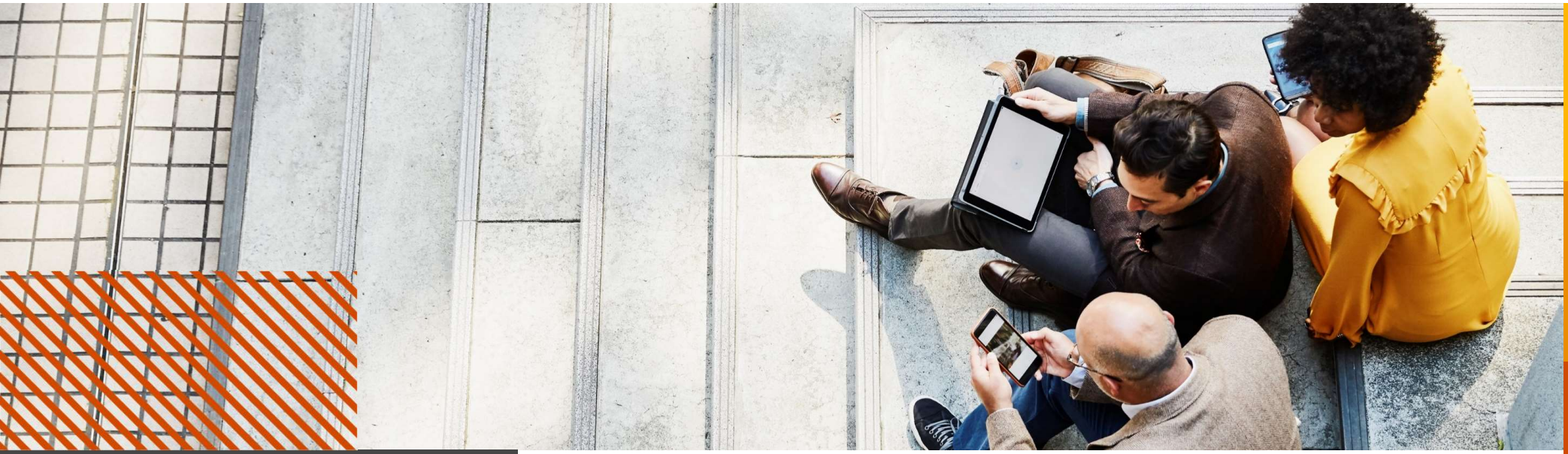


Table of contents

Introduction

01

Introduction

On 30 April 2024, the Reserve Bank of India (RBI) released an updated Guidance Note on Operational Risk Management and Operational Resilience.[1] The regulator has made major changes to the now repealed Guidance Note on Management of Operational Risk dated 14 October 2005. The guidelines brings the Basel Committee on Banking Supervision (BCBS) Principles and international best practices into line with RBI rules.

The guidance note's introduction stresses on effective operational risk management for all financial sector regulated entities (REs). It demonstrates how interruptions to operations may affect consumers, jeopardise the sustainability of an RE and upset financial stability. The many operational risks that REs encounter are described in the beginning, including those pertaining to people, process, technology and external events. Finally, it highlights how proactive identification, evaluation and management of these risks by REs is essential for operational resilience.

Operational risk and resiliency management global milestones

2021

Basel Committee highlighted operational resilience as the outcome of operational risk management

2022

Prudential Regulation Authority of UK published a statement of policy on operational resilience, defining its relationship with operational risk

2023

Australian Prudential Regulation Authority published its revised operational risk management standard, including resilience requirements

2024

Reserve Bank of India issued a revised guidance note on operational risk management combining it with operational resiliency

Applicability

- Commercial banks
- Primary (urban) co-operative banks/state co-operative banks/central co-operative banks
- All-India financial institutions (viz. Exim Bank, National Bank For Agriculture and Rural Development (NABARD), National Housing Bank (NHB), Small Industries Development Bank of India (SIDBI), National Bank for Financing Infrastructure and Development (NaBFID))
- All non-banking financial companies, including housing finance companies

[1] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12679&Mode=0

Three pillars of the guidance note

Pillar I

Prepare and Protect

- Three lines of defense (LoDs) for management of operational risk
- Governance and risk culture
- Monitoring and reporting
- Responsibilities of board of directors (BoD) and senior management
- Risk management environment – identification and assessment
- Control and mitigation
- Change management

Covering 9 underlying principles

Pillar II

Build resilience

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

Covering 6 underlying principles

Pillar III

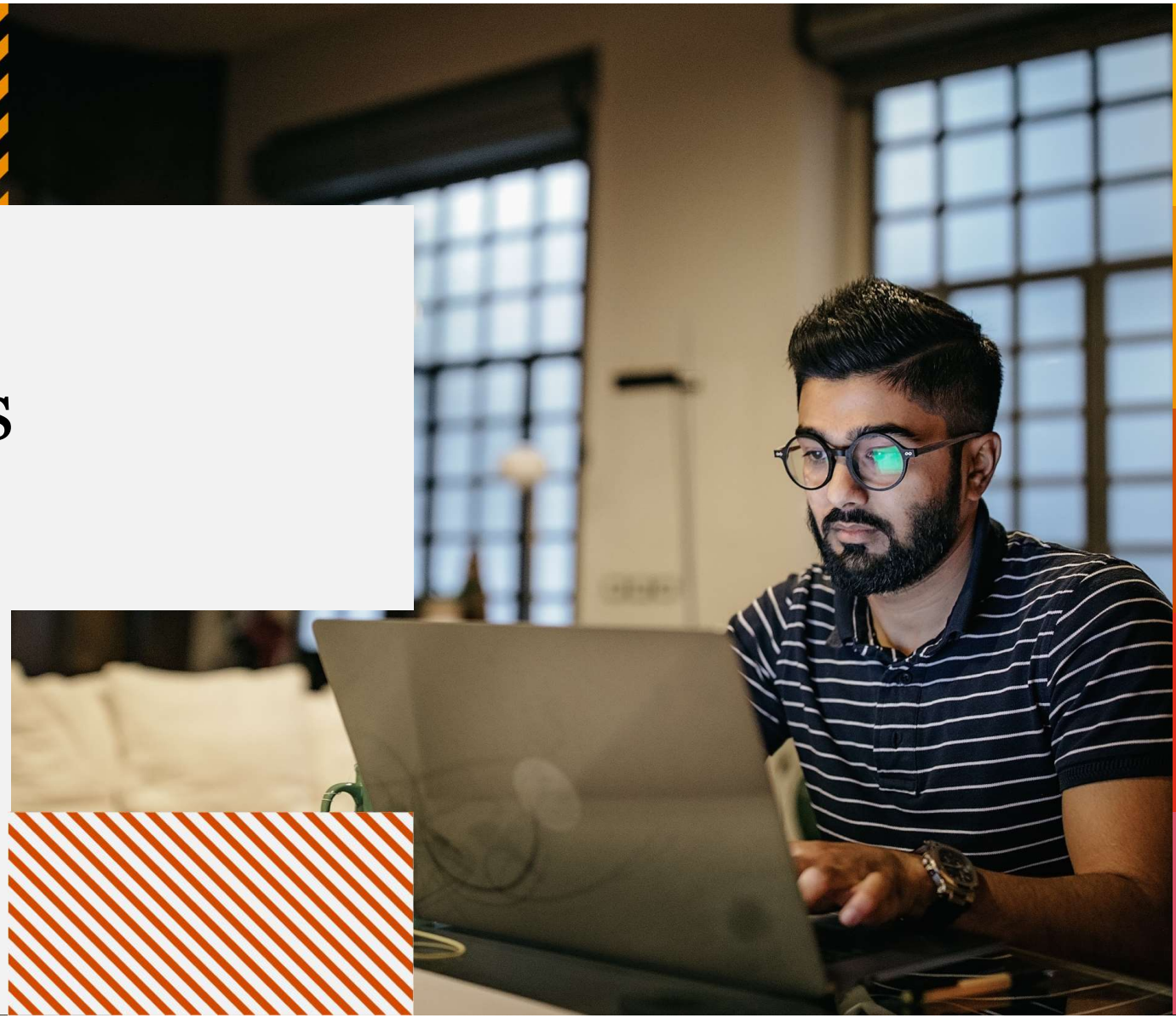
Learn and Adapt

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

Covering 3 underlying principles

Key highlights

02



Pillar I: Prepare and Protect (1/3)

Prepare and Protect

Governance and risk culture

Operational risk management framework (ORMF) to cover:
- Governance structure, policies and procedures, risk appetite & tolerance, tools for risk and control identification
- Approach to ensure controls are designed, implemented and operate effectively
- Risk and controls inventory, risk reporting and, common taxonomy of operational risk terms.
- Independent review and challenge of the outcomes of the risk management process, methodology incl benchmarking and comparative analysis

Integrated ORMF should be embedded across all levels including group and business units as well as new business initiatives, products, services, activities, processes and systems

ORMF governance structure to be commensurate with the nature, size, complexity and risk profile of entity's activities, including committee structure, composition and entity's operation

Responsibilities of BoD and senior management

Three LoDs to be defined in the ORMF:
- Business unit – 1st LoD
- Organisational ORM function and compliance Function – 2nd LoD
- Audit function – 3rd LoD)

Roles and responsibilities of the three LoDs should be defined as below:
- **1st LoD:** ORMF to be integrated into the overall risk management process. Focus on risk identification and assessment, establishment of controls to mitigate risks, monitoring and reporting of operational risk profiles.
- **2nd LoD:** Focus on building governance and risk culture, developing an independent view regarding business unit's risk profile, challenging the relevance and consistency of the business unit's implementation of the ORM tools.
- **3rd LoD:** Focus on providing independent assurance to the board regarding the overall adequacy and appropriateness of the ORMF and the governance processes.

Three LoDs for management of operational risk

Results of the operational risk assessment to be incorporated into overall business strategy development process

Governance and controls to be adequate and factor in risks arising from incentive arrangements

Board is responsible and accountable for oversight over ORMF and also for performing regular review and evaluation of effectiveness of ORMF

Board to set the tone at the top with strong culture of risk management and ethical business practices

Board-approved risk appetite for operational risk and resiliency and tolerance statement should be forward-looking and linked with short- and long-term strategic and financial plans

Establish a code of conduct (CoC)/ethics policy for both staff and board members and periodic attestation by employees.
CoC to be available on the entity's website

Segmented operational risk training based on the seniority, role and responsibilities of the individuals

Pillar I: Prepare and Protect (2/3)

Prepare and Protect

Identification and assessment

Focus on effective risk identification and assessment through operational risk tools:

- **Self-assessment:** Consideration of quantitative and qualitative elements in self-assessment; analysis of events and using this information as an input to the risk control self-assessment
- **OR event data and event management:** Understanding the underlying causes of events and control weaknesses, and formulating an appropriate response to prevent recurrence
- **Control monitoring and assurance framework:** Monitoring to include analysis of control design and operating effectiveness and sufficiency of control coverage
- **Robust monitoring of metrics:** Key risk indicators and linkage with associated risk and controls
- **Scenario analysis:** Consider internal and external loss data, information from self-assessments, the control monitoring and assurance framework, forward-looking metrics, root-cause analyses and the process framework. Ensure scenario and stress testing for the risk appetite.

Control and mitigation

Control environment should be a combination of controls pertaining to segregation of duties, other traditional internal controls and technology implementation (automated controls)

Controls processes and procedures to address how the regulated entity (RE) ensures continuity of operations in both normal circumstances and in the event of disruption

Risk mitigation strategy to focus on treating or terminating the risk or transferring the risk to another party such as through insurance. Assess whether such insurance truly reduces risk, or creates a new risk (e.g. counterparty risk)

Monitoring and reporting

Reports on operational risk should be comprehensive, accurate, consistent and action oriented and provide an outlook on operational risk profile across business units and products, and ensure adherence to operational risk appetite and tolerance statement at bank level

Updates on operational risk profile should take into account parameters such as internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions; results of operational risk monitoring activities should be reported to board, including internal/external assessments of the ORMF

Results of operational risk monitoring activities should be reported to board, including internal/external assessments of the ORMF

Pillar I: Prepare and Protect (3/3)

Prepare and Protect

Change management

Clear allocation of roles and responsibilities in change management, in accordance with the three LOD model

Change management to assess the evolution of associated risks across time, from inception to termination

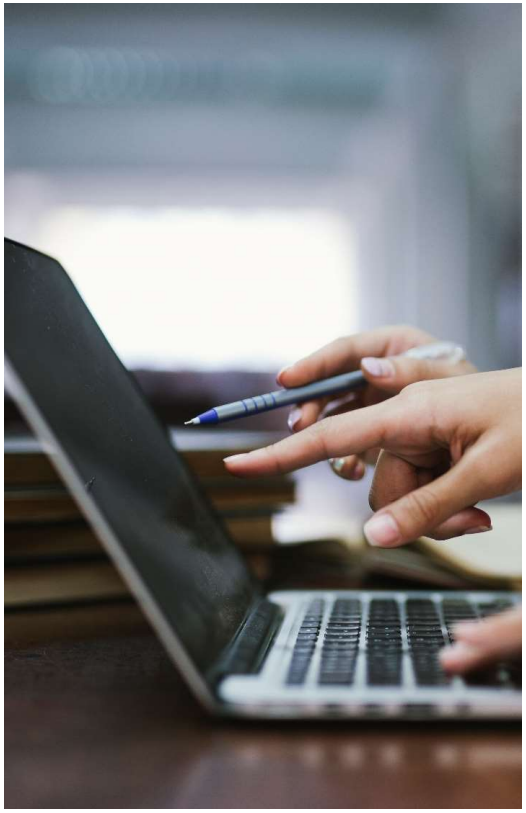
Policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change on the basis of agreed objective criteria

Changes should be monitored, during and after their implementation

Policies and procedures for the review and approval of new products, services, activities, processes and systems

Maintenance of a central record of products and services (including third-party arrangements)

Appropriate investment to be made for human resources and technology infrastructure before changes are introduced



Pillar II: Build Resilience (1/2)

Build Resilience

BCP and testing	Assessment of interconnections and interdependencies	Third-party dependency management
Dedicated vertical for management of operational resilience in the 1st and 2nd LoD and technology platform for end-to-end management of operational resilience		Put in place policies and procedures for business continuity and disaster recovery
Operational resiliency to be explicitly in charter of RMC of the board and ORMC of executives		Recovery and resolution plan detailing critical operations, systems and technology, outsourced partners and independencies and interconnections
Build operational resilience approach considering the risk appetite and tolerance for disruption to its critical operation and operational capabilities		Third-party due diligence to include resilience assessment, contingency plan and nth party assessment
Clearly define and document criteria to determine how operations are classified as critical and non-critical from an operational resiliency perspective		While contracting with a third party, clearly call out responsibility for resilience and ensure nth party risk management
Impact tolerance metric for each of the entity's critical operations which may be time based, quantity based or service level, to quantify the maximum acceptable level of disruption		BCP planning and infrastructure should be commensurate to risk appetite and envisaged contingency scenarios
Allocate financial, technical and other resources by senior management to support the overall operational resilience approach, ensuring staff with sufficient stature and experience		Recovery and resolution plan should clearly detail triggers for invocation, testing programmes, training and awareness, communication and crisis management

Pillar II: Build Resilience (3/2)

Build Resilience

Third-party dependency management

- BCP plan should be tested for its efficacy and effectiveness involving people, process, technology and third parties
- Continuously improve response to crisis and recovery plan based on learnings from previous incident and simulation of various scenarios
- Crisis management team with authority should be put in place for internal management of contingency and external reporting and communication
- Information communication technology (ICT) cybersecurity risk management should be fully integrated with overall operational resiliency
- ICT policy detailing governance, information assets, risk ownership and accountability, cybersecurity tools and security measures, periodic evaluation and monitoring of cybersecurity controls and incident response

Incident management and continuous improvements

ICT and cybersecurity

- Inventory and risk assessment of critical information, assets and infrastructure as part of ICT risk management
- ICT and cybersecurity risk mitigation and fallback plan proportionate to assessed risk level
- Well laid out and tested ICT response and recovery programme, change management, incident management
- ICT readiness building and testing for disruptive external events such as remote access, deployment of physical assets, remote user connection, etc.
- Board and senior management oversight over effectiveness of ICT risk management proportionate to threat levels and continuous improvement based on external and internal control environment
- Operational resilience to be a fundamental element of any strategic decision taken as part of designing of products and services

Pillar III: Learn and Adapt

Learn and Adapt

Disclosure and reporting	Lessons learned exercise and adapting	Continuous improvement through feedback systems
Put in place operational risk disclosure policy approved by senior management and BoD	Conduct a 'lessons learned exercise', including root cause analysis after any disruption to a business service with emphasis on critical service, including third-party service provider	RE to learn from its experiences as changes to its operational approaches or technology infrastructure mature over time
Disclose relevant operational risk exposure information to the stakeholders (including significant operational loss events), while not creating operational risk through this disclosure	Define predetermined criteria or questions to identify deficiencies which caused induced failure in the continuity of service and these deficiencies should be addressed as a matter of priority	Promote an effective culture of learning and continuous improvement as operational resilience evolves
Disclose ORMF in a manner that allows stakeholders to determine whether the RE identifies, assesses, monitors and controls/mitigates operational risk effectively	The lessons learned exercises to define effective remediation measures to redress deficiencies and failure in the continuity of service	Continuous feedback loop: Identify/assess the type, nature and severity of potential operational risks → required set of control/mitigation measures developed → operational incidents/disruptions occurred
Disclosures to allow REs to undertake a peer-to-peer comparative analysis for improving their own processes and controls		

Conclusion: Focus on a robust and resilient financial sector

A stepping stone

Important circular and a stepping stone clearly calling out the contours of Operational Risk Management framework, Operational Risk is not about 2nd LOD but should be embedded in 1st LOD process design and linking the same to resilience across REs

Setting the tone at the top

The actions of BoD and senior management as well as the RE's risk management policies, processes and systems provide the foundation for a sound risk management culture.

Risk management environment

Managing the end-to-end review cycle effectively is critical for a sound risk management environment which covers 'risk identification-control assessment-mitigation-monitoring-reporting'.

Recognizing change management as distinct topic for strengthening of operational risk and resiliency

Prepare, respond, recover

An operational resilience approach should be built considering the risk appetite and tolerance for disruption to its critical operation and its operational capabilities.

Operational resilience to be a fundamental element of any strategic decision taken as part of designing of products and services .

Learn, adapt and improve on continuous basis

Learning from past instances, adapting to changes and accordingly re-defining and improving processes is a continuous process.

Way forward

03

Assess the current state and build a working group

Key Actions	Key activities to be performed
Assess the current state and build a working group	• Assess the current maturity of the organization vis-à-vis the requirements of the RBI's guidelines on operational risk and develop action plan for compliance. • The action plan may be bifurcated into the short term and medium term, covering the need for strengthening operational risk within the 1st LoD, a separate function for operational resiliency, change management, governance structure, policies and procedures, technology enhancements and people allocation. • Set up a working group which may consist of the operational risk head, and representatives of various 1st LoD functions and support functions such as information security, human resource, finance and corporate communications.
Perform gap assessment and define an action plan along with action owner	• While assessing the current state, identify the gaps in the governance framework, technology implementation and resource allocation. • Prepare an inventory of the relevant existing policies and procedures and perform a gap assessment with the desired state. • Review the current technology and assess the need for technology enhancements to achieve the desired state. • Review the current resource allocation from the number, stature and experience perspective and perform a gap assessment with resource requirement of the desired state. • Put in place an action plan after discussion with the working group and decide an action owner from the working group.

Build/refresh governance framework

Key Actions	Key activities to be performed
 **Build/refresh the governance framework**	**Build/refresh the governance framework focusing on the following aspects:** • Board to be responsible for building the governance framework, approval of policies and procedures, and providing continuous oversight over the implementation of the policies and procedures the laid down. • Build a strong culture of risk management and ethical business practices. • Build a three LoD framework and demonstrate its implementation and satisfactory operation. • Put in place appropriate committee structure and committee composition. • Build a comprehensive operational risk management framework focusing on governance structure, policies and procedures, risk appetite, and tolerance statement and tools for operational risk management. • Build a change management governance framework in the 1st and 2nd LoD, policies and procedures. • Build an operational resilience governance framework in the 1st and 2nd LoD and its approach considering the risk appetite and tolerance for disruption to its critical operation and its operational capabilities. • Put in place clearly defined and documented criteria to determine how operations are classified as critical and define the impact tolerance metric for each of its critical operations which may be time, quantity or service level based, to quantify the maximum acceptable level of disruption. • Build a continuous feedback loop on occurrence of any incident, resulting in continuous improvement. • Ensure incorporation of results of the operational risk assessment into the overall business strategy development process, with operational resilience to be a fundamental element of any strategic decision taken by the RE.

Build/refresh policies and procedures and manage people

Key Actions	Key activities to be performed
Build/refresh policies and procedures	**Build/refresh the following policies/procedures:** • Operational risk management policy, including operational resiliency • Operational risk and resiliency governance framework • Governance committees and its terms of reference at the executive and board level • Risk appetite and tolerance statement • Risk control self-assessment procedure • Operational risk event loss data and event management procedure • Key risk indicators/metrics monitoring procedure • Scenario analysis and stress testing procedure • Benchmarking and comparative analysis procedure • CoC/ethics policy for both staff and board members • Change management policy • Product and process approval policy • Vendor management framework • Business continuity planning policy, including testing • Recovery and resolution plan • Crisis management plan and team • ICT and cybersecurity policy • Disclosure policy
Manage people/ human resources	• Put in place segmented operational risk training based on the seniority, role and responsibilities of the individuals. • Ensure allocation of financial, technical and other resources by senior management to support the overall operational risk management framework, including operational resilience, along with ensuring staff with sufficient stature and experience. • Ensure appropriate investment in human resources before any new changes are introduced.

Technology enhancements and other key actionables

Key Actions	Key activities to be performed
Technology enhancements	• Focus on technology implementation (automated controls) while building the control environment. • Ensure appropriate investment in technology infrastructure before any changes are introduced. • Build a technology platform for end-to-end management of operational resilience.
Other key actionables	• Build reports on operational risk which are comprehensive, accurate, consistent and action-oriented and provide an outlook on operational risk profile across business units and products. • Put in place a risk mitigation strategy focusing on treating the risk, terminating the risk or transferring the risk to another party such as through insurance. • Include resilience assessment, contingency plan and nth party assessment in third-party due diligence . • Maintain a central record of products and services to the extent possible (including the third-party arrangements). • Disclose relevant operational risk exposure information to stakeholders (including significant operational loss events).

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Rounak Shah
Partner
M: +91 98209 84358
E: rounak.shah@pwc.com

Amol Bhat
Partner
M: +91 98232 64158
E: amol.bhat@pwc.com

Thank you

PR – June 2024 – M&C 38121