भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

Guidance Note on Operational Risk Management and Operational Resilience

RBI/2024-25/31
DOR.ORG.REC.21/14.10.001/2024-25 April 30, 2024

1. Purpose

1.1 Operational Risk is inherent in all banking/ financial products, services, activities, processes, and systems. Effective management of Operational Risk is an integral part of the Regulated Entities' (REs) risk management framework. Sound Management of Operational Risk shows the overall effectiveness of the Board of Directors and Senior Management in administering the RE's portfolio of products, services, activities, processes, and systems.

1.2 An operational disruption can threaten the viability of an RE, impact its customers and other market participants, and ultimately have an impact on financial stability. It can result from man-made causes, Information Technology (IT) threats (e.g., cyber-attacks, changes in technology, technology failures, etc), geopolitical conflicts, business disruptions, internal/external frauds, execution/ delivery errors, third party dependencies, or natural causes (e.g., climate change, pandemic, etc.).

1.3 An RE needs to factor in the entire gamut of risks (including the aforesaid risks in its risk assessment policies/ processes), identify and assess them using appropriate tools, monitor its material operational exposures and devise appropriate risk mitigation/management strategies using strong internal controls to minimize operational disruptions and continue to deliver critical operations, thus ensuring operational resilience.

1.4 Until recently, the predominant Operational Risks that REs faced emanated from vulnerabilities related to increasing dependence and rapid adoption of technology for provision of financial services and intermediation. However, the

विनियमन विभाग, केंद्रीय कार्यालय, केंद्रीय कार्यालय भवन, 12वीं/13वीं मंजिल, शहीद भगत सिंह मार्ग, फोर्ट, मुंबई - 400001
टेलीफोन/ Tel No: 22661602, 22601000 फैक्स/ Fax No: 022-2270 5691 Email: cgmicdor@rbi.org.in
Department of Regulation, Central Office, Central Office Building, 12th/ 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai – 400001

financial sector's growing reliance on third-party providers (including technology service providers) exacerbated by Covid-19 pandemic with greater reliance on virtual working arrangements, has highlighted the increasing importance of Operational Risk Management and Operational Resilience; which not only benefits the RE by strengthening its ability to remain a viable going concern but also supports the financial system by ensuring continuous delivery of critical operations during any disruption.

1.5 In view of the foregoing, the Reserve Bank, through this Guidance Note on Operational Risk Management and Operational Resilience (hereafter 'Guidance Note') intends to:

1.5.1 promote and further improve the effectiveness of Operational Risk Management of the REs, and

1.5.2 enhance their Operational Resilience given the interconnections and interdependencies, within the financial system, that result from the complex and dynamic environment in which the REs operate.

1.6 This Guidance Note updates the "Guidance Note on Management of Operational Risk" dated October 14, 2005. It has been prepared based on the Basel Committee on Banking Supervision (BCBS) principles documents issued in March 2021, viz., (a) 'Revisions to the Principles for the Sound Management of Operational Risk' and (b) 'Principles for Operational Resilience' as well as the some of the international best practices.

1.7 The Guidance Note has adopted a principle-based and proportionate approach to ensure smooth implementation across REs of various sizes, nature, complexity, geographic location and risk profile of their businesses. Although the exact approach may vary from RE to RE, the Guidance Note provides an overarching guidance to REs for improving and further strengthening their Operational Risk Management Framework (ORMF). It gives adequate flexibility to REs for Operational Risk Management to enhance their ability to withstand, adapt and recover from potential operational disruptions and ensure their Operational Resilience. The systems, procedures and tools prescribed in this Guidance Note are indicative in nature and should be read in conjunction with the relevant instructions issued by Reserve Bank from time to time. In case of inconsistency, if any, the relevant instructions issued by the Reserve Bank would prevail.

1.8 The operational risk regulatory capital requirements shall continue to be guided by the applicable guidelines[1].

2. Application

2.1 This Guidance Note shall apply to the following REs:

2.1.1 All Commercial Banks[2];

2.1.2 All Primary (Urban) Co-operative Banks/State Co-operative Banks/Central Co-operative Banks;

2.1.3 All All-India Financial Institutions (viz., Exim Bank, NABARD, NHB, SIDBI, and NaBFID); and

2.1.4 All Non-Banking Financial Companies including Housing Finance Companies.

3. Repeal and Transitional Arrangements

With the issuance of this Guidance Note the "Guidance Note on Management of Operational Risk" dated October 14, 2005, stands repealed.

4. Key changes

Key changes carried out in this Guidance Note vis-à-vis the repealed Guidance Note are given in Annex.

Yours faithfully,

(Sunil T. S. Nair)
Chief General Manager

[1] The approach for operational risk capital calculation for banks is detailed in "Master Circular – Basel III Capital Regulations" dated April 1, 2024, as amended from time to time. However, REs such as Small Finance Banks, Payments Banks, Regional Rural Banks, Local Area Banks, NBFCs, and Co-operative Banks are not required to maintain separate regulatory capital for operational risk.

[2] "Commercial Banks" means all banking companies, corresponding new banks, Regional Rural Banks and State Bank of India as defined under subsections (c), (da), (ja) and (nc) of Section 5 of the Banking Regulation Act, 1949. This also includes banks incorporated outside India and licensed to operate in India ('Foreign Banks'), Local Area Banks, Payments Banks, and Small Finance Banks.

Guidance Note on Operational Risk Management and Operational Resilience

Index

Sr. No.	Subject	Page No.
1.	Preliminary – Introduction and Background	2
2.	Definitions	4
3.	Three lines of Defence for management of Operational Risk	7
4.	Governance and Risk Culture	11
5.	Responsibilities of Board of Directors and Senior Management	15
6.	Risk management environment - Identification and assessment	21
7.	Change Management	25
8.	Monitoring and Reporting	27
9.	Control and Mitigation	28
10.	Essential Elements of Operational Resilience	31
11.	Mapping of Interconnections and Interdependencies	32
12.	Third-party dependency management	33
13.	Business Continuity Planning and Testing	35
14.	Incident management	37
15.	Information and Communication Technology (ICT) including cyber security	38
16.	Disclosure and Reporting	41
17.	Lessons Learned Exercise and Adapting	42
18.	Continuous improvement through Feedback Systems	43
19.	Annex	45

1. PRELIMINARY

1.1 Introduction

1.1.1 The global financial crisis greatly impacted financial stability around the world. Given the fact that the effects of crisis were much more severe than all the scenarios envisaged by banks as part of their stress tests, several structural changes were undertaken to strengthen banks'/financial institutions' financial resilience. Though capital and liquidity requirements have improved the ability of banks to absorb shocks, Basel Committee on Banking Supervision (BCBS) was of the view that more work needs to be done in the area of Operational Risk Management to provide additional safeguards to the financial system.

1.1.2 The BCBS recognized Operational Risk as a distinct class of risk in 2001, outside of credit and market risks and came out with Sound Practices for Management and Supervision of Operational Risk in 2003. Subsequently, these principles were revised in 2011, to incorporate the lessons learnt from the Great Financial Crisis of 2007-09. In 2014, a review of the implementation of these Principles was carried out to assess the extent to which banks had implemented these Principles, identify significant gaps, if any, in their implementation and highlight emerging and noteworthy Operational Risk Management practices at banks which may be included in the Principles. It was also observed that several Principles have not yet been adequately implemented, and there was a need for further guidance to facilitate their implementation in areas such as risk identification and assessment tools, key risk indicators, business process mapping, monitoring of action plans, change management programmes and processes, implementation of the three lines of defence, oversight by Board of Directors and Senior Management, articulation of Operational Risk appetite and tolerance statements, risk disclosures, etc. BCBS also recognised that the 2011 Principles did not adequately capture certain important sources of Operational Risk, such as those arising from Information and Communication Technology (ICT) risk.

1.1.3 Subsequently, the onset of Covid-19 pandemic created disruptions affecting information systems, personnel, facilities, relationships with third-party service providers and customers. It altered the way banks operated in view of their increased demands on technology given the greater reliance on virtual working arrangements. In addition, incidents of cyber threats (ransomware attacks, phishing, etc.) spiked,

and the likelihood for materialising of the Operational Risk events caused by people, failed processes, and systems increased, which tested the operational resilience of banks.

1.1.4 In light of the same, BCBS felt that further work was necessary to strengthen banks' ability to withstand Operational Risk related events such as pandemics, cyber incidents, technology failures and natural disasters which could cause significant operational failures or widespread disruptions in financial markets. It is in this backdrop, that BCBS came out with updated 'Principles for the Sound Management of Operational Risk' in 2021. Additionally, it also came out with 'Principles on Operational Resilience' to enhance the ability of banks to withstand, adapt to and recover from potential hazards.

1.2 Background

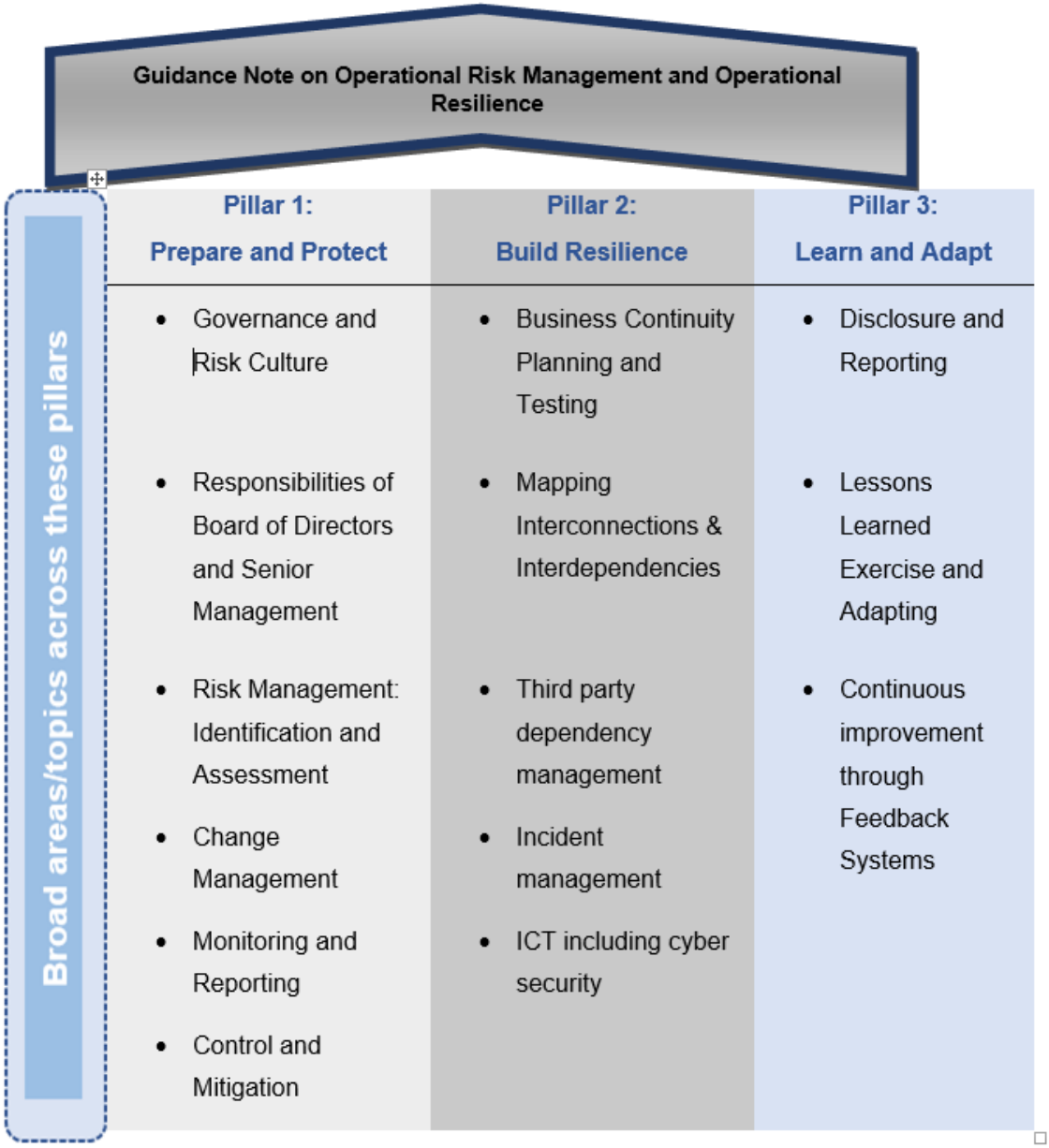
1.2.1 Operational Risk is a complex risk category, when it comes to identification, quantification and mitigation of risk. It is impacted by numerous factors such as internal business processes, regulatory landscape, business growth, customer preferences, and even factors external to the organization. It is highly dynamic in nature where new and emerging forces such as breakthrough technologies, data availability, new business models, interaction with third parties, etc., continuously create new demands on Operational Risk Management Framework (ORMF).

1.2.2 While Operational Risk Management allows an RE to better identify, assess and mitigate the Operational Risks, Operational Resilience provides it 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 a robust level of Operational Resilience work together to reduce the frequency and the impact of Operational Risk events. In view of the above, Reserve Bank, through this Guidance Note intends to promote Operational Risk Management and enhance the Operational Resilience of REs.

1.2.3 This Guidance Note on Operational Risk Management and Operational Resilience has been built on three pillars. The three pillars are:

(i) Prepare and Protect
(ii) Build Resilience

(iii) Learn and Adapt



1.2.4 These three pillars support a holistic approach to the management of Operational Risk and Operational Resilience and create a feedback loop that fosters perpetual embedding of lessons learned into an RE's preparation for operational disruptions and its performance during actual occurrence of disruptions.

Across these three pillars, the Guidance Note contains 17 principles detailed hereafter in paragraphs 4-18.

2. Definitions

2.1 "Business unit" is responsible for identifying and managing the risks inherent in the products, services, activities, processes and systems for which it is

accountable and includes all associated support, corporate and/or shared service functions, e.g., Finance, Human Resources, and Operations and Technology. It does not include Risk Management and Internal Audit functions unless otherwise specifically indicated**.**

2.2 "**Critical operations**" refers to critical functions[3], activities, processes, services and their relevant supporting assets[4] the disruption of which would be material to the continued operation of the RE or its role in the financial system. Whether a particular operation is "critical" depends on the nature of the RE and its role in the financial system. REs' tolerance for disruption should be applied at the critical operations level.

2.3 **"Event management"** is the process of identification, analysis, end-to-end management and reporting of an operational risk event that follows a pre-determined set of protocols.

2.4 "**Incidents**" are current or past disruptive events the occurrence of which would have an adverse effect on critical operations of the RE. Incident management is the process of identifying, analysing, rectifying and learning from an incident (including a cyber incident) and preventing recurrences or mitigating the severity thereof. The goal of incident management is to limit the disruption and restore critical operations in line with the RE's risk tolerance for disruption.

2.5 "**Information and Communication Technology**"[5] refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environment.

2.6 "**Mapping**" is the process of identifying, documenting, and understanding the chain of activities involved in delivering critical operations. It incorporates the

---

[3] According to the Financial Stability Board (FSB), *critical functions* are defined as "activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the RE's group size or market share, external and internal interconnectedness, complexity and cross-border activities. Examples include payments, custody, certain lending and deposit-taking activities in the commercial or retail sector, clearing and settling, limited segments of wholesale markets, market making in certain securities and highly concentrated specialist lending sectors." (FSB's guidance on '*Recovery and resolution planning for systemically important financial institutions: guidance on identification of critical functions and critical shared services'*, dated July 16, 2013)

[4] In this context, "supporting assets" are defined as people, technology, information and facilities necessary for the delivery of critical operations.

[5] As per the National Institute for Standards and Technology (NIST), USA, Information and Communications Technologies (ICT) encompasses all technologies for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and information.

identification of all interdependencies and interconnections including people, processes, technology and third parties.

2.7 "**Operational resilience**" means the ability of an RE to deliver critical operations through disruption. This ability enables an RE to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, an RE should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption or impact tolerance.

2.8 "**Operational Risk"** means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. It includes legal risk but excludes strategic and reputational risk and it is inherent in all banking/ financial products, activities, processes and systems.

2.9 "**Operational Risk Management"** Operational Risk Management refers to entire gamut of activities right from risk identification, measurement and assessment, monitoring and control, mitigation, reporting to senior management and the Board of Directors on the RE's risk exposures, Business Continuity Management, and learning through feedback for improvement.

2.10 "Operational Risk profiles" describe the Operational Risk exposures and control environment assessments of business units of REs and it considers the range of potential impacts that could arise from estimates of expected to plausible severe losses.

2.11 "**Regulated Entities**" (REs) refers to the entities mentioned below:

2.11.1 All Commercial Banks[6];

2.11.2 All Primary (Urban) Co-operative Banks/State Co-operative Banks/Central Co-operative Banks;

2.11.3 All All-India Financial Institutions (AIFIs) (viz., Exim Bank, NABARD, NHB, SIDBI, and NaBFID); and

[6] "Commercial Banks" means all banking companies, corresponding new banks, Regional Rural Banks and State Bank of India as defined under subsections (c), (da), (ja) and (nc) of Section 5 of the Banking Regulation Act, 1949. This also includes banks incorporated outside India licensed to operate in India ('Foreign Banks'), Local Area Banks, Payments Banks, and Small Finance Banks.

2.11.4 All Non-Banking Financial Companies (NBFCs) including Housing Finance Companies.

2.12 "**Respective functions**" refers to the appropriate function(s) within the RE's three lines of defence, which are (i) business unit management; (ii) an independent Operational Risk Management including Compliance function; and (iii) audit function.

2.13 "**Risk appetite**" is the aggregate level and types of risk an RE is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.[7]

2.14 **"Risk tolerance"** is the variation around the prescribed risk appetite that the RE is willing to tolerate.

2.15 "**Supervisory Authority**" means,

2.15.1 Reserve Bank of India in case of Commercial Banks (including Local Area Banks, Payments Banks, Small Finance Banks, and Primary Urban Co-operative Banks), Non-Banking Financial Companies, and All India Financial Institutions.

2.15.2 National Bank For Agriculture And Rural Development (NABARD) in case of State Co-operative Banks, Central Co-operative Banks, and Regional Rural Banks.

2.15.3 National Housing Bank (NHB) in case of Housing Finance Companies.

2.16 "**Tolerance for disruption or Impact Tolerance**" is the level of disruption from any type of Operational Risk an RE is willing to accept given a range of severe but plausible scenarios.

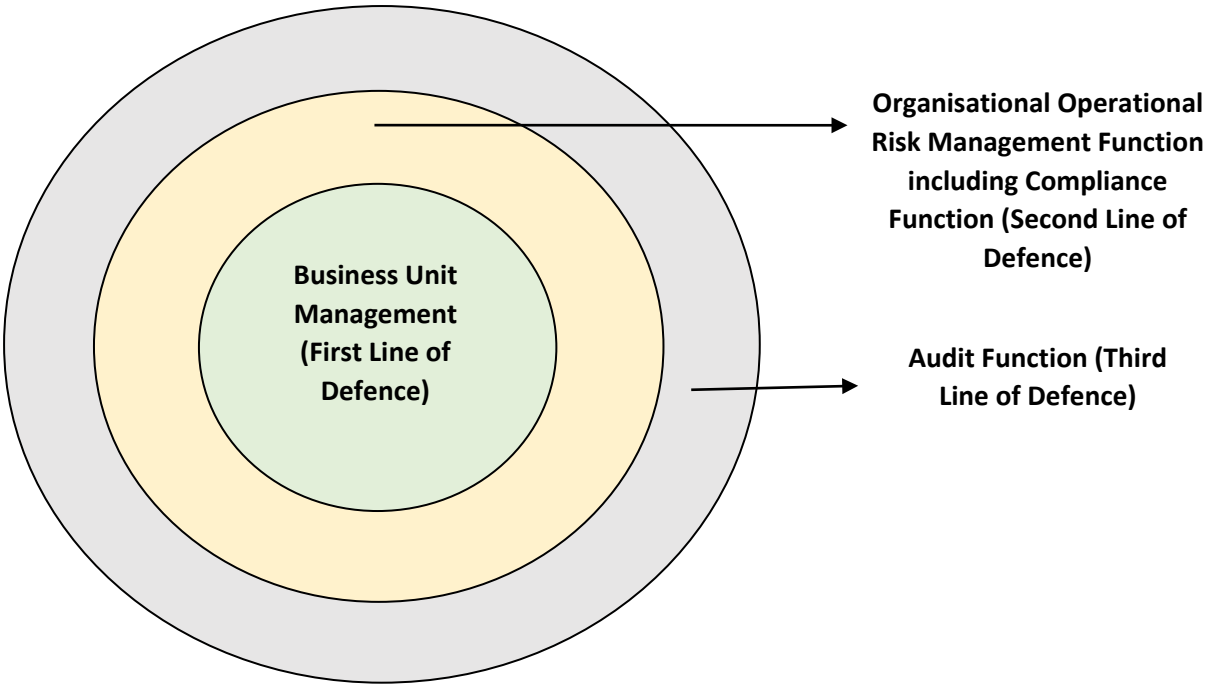
PILLAR I: Prepare and Protect

3. Three lines of defence for management of Operational Risk

3.1 Sound internal governance forms the foundation of an effective ORMF. The Operational Risk governance function of REs should be fully integrated into their overall risk management governance structure. REs may leverage their existing risk management functions for this purpose.

[7] "Risk appetite" is defined in BCBS's 2015 Corporate governance guidelines, which use the FSB's 2013 Principles for an effective risk appetite framework.

3.2 As a part of their ORMF, REs shall rely on three lines of defence:



3.2.1 First line of Defence

3.2.1.1 Business Unit Management typically forms the first line of defence. Sound Operational Risk governance recognises that business unit management is responsible for identifying and managing the risks inherent in the products, services, activities, processes and systems for which it is accountable. REs should have a policy that defines clear roles and responsibilities of relevant business units. The responsibilities of an effective first line of defence in promoting a sound Operational Risk Management culture should include:

(i) Identifying and assessing the materiality of Operational Risks inherent in their respective business units through the use of Operational Risk Management tools;

(ii) Establishing appropriate controls to mitigate inherent Operational Risks, and assessing the design and effectiveness of these controls through the use of the Operational Risk Management tools;

(iii) Reporting whether the business units lack adequate resources, tools and training to ensure identification and assessment of Operational Risks;

(iv) Monitoring and reporting the business units' Operational Risk profiles, and ensuring their adherence to the established Operational Risk appetite and tolerance statement; and

(v) Reporting residual Operational Risks not mitigated by controls, including operational loss events, control deficiencies, process inadequacies, and non-compliance with Operational Risk tolerances.

3.2.2 Second line of defence

3.2.2.1 A functionally independent Organisational Operational Risk Management Function (OORF) forms the second line of defence. The responsibilities of an effective second line of defence in promoting a sound Operational Risk Management culture should include:

(i) Developing an independent view regarding business units' (a) identified material Operational Risks, (b) design and effectiveness of key controls, and (c) risk tolerance;

(ii) Challenging the relevance and consistency of the business unit's implementation of the Operational Risk Management tools, measurement activities and reporting systems, and providing evidence of this effective challenge;

(iii) Developing and maintaining Operational Risk Management and measurement policies, standards and guidelines;

(iv) Reviewing and contributing to the monitoring and reporting of the Operational Risk profile; and

(v) Designing and providing Operational Risk training and instilling risk awareness.

3.2.2.2 At smaller REs (i.e., NBFC-Base Layer and Tier 1 & 2 Co-operative Banks for the purpose of this Guidance Note), if functions of both first and second line of defence are carried out by the same unit, independence may be achieved through separation of duties (with documented policies and processes emphasizing the same) and an independent review of processes and functions. In larger REs (i.e., REs other than the smaller REs), the OORF should have a reporting structure independent of the risk-generating business units and be responsible for the design, maintenance and ongoing development of the ORMF within the RE. The OORF typically engages relevant corporate control groups (e.g., Legal, Finance and IT) as well as the overall Risk Management Function of the RE, to support its assessment of the Operational Risks and controls. REs should have a policy which clearly defines the roles and responsibilities of the OORF, reflective of the size and complexity of the organisation.

3.2.2.3 In addition to the independent ORMF, the second line of defence also typically includes the compliance function.

3.2.3 Third line of defence

The third line of defence, i.e the audit function provides an independent assurance to the Board regarding the appropriateness of RE's ORMF. This function's staff should not be involved in the development, implementation and operation of Operational Risk Management processes which has been carried out by the other two lines of defence. The third line of defence reviews are generally carried out by RE's internal and/or external audit but may also involve suitably qualified independent third parties. The scope and frequency of reviews should not only be sufficient to cover all activities and legal entities of an RE, aligned with the RE's Operational Risk profile, and identify and prioritize key risk areas that warrant thorough examination but also be responsive to the dynamic nature of the Operational Risk environment. An effective independent review includes two processes:

3.2.3.1 Validation

Ensuring that the quantification systems used by the RE are sufficiently robust as (i) they provide assurance about the integrity of inputs, assumptions, processes and methodologies and (ii) results in assessment of Operational Risk that credibly reflects the Operational Risk profile of the RE;

3.2.3.2 Verification

(i) Review of the design and implementation of the Operational Risk Management systems (including compliance and consistency with Board policies) and associated governance processes through the first and second lines of defence (including the independence of the second line of defence);
(ii) Review of validation processes to ensure they are independent and implemented in a manner consistent with established RE policies;
(iii) Ensuring that business units' management promptly, accurately and adequately responds to the issues raised, and regularly reports to the Board of Directors or its relevant Committees on pending and closed issues;
(iv) Identifying gaps, if any, in the ORMF and reporting to the Board or its relevant Committee; and

(v) Providing opinion on the overall adequacy and appropriateness of the ORMF and the associated governance processes across the RE by assessing whether the ORMF meets organisational needs and expectations (such as in respect of the risk appetite and tolerance, and adjustment of the framework to changing circumstances) and complies with statutory and legislative provisions, contractual arrangements, internal rules and ethical conduct.

3.3 REs should ensure that each line of defence:

3.3.1 has clearly defined roles and responsibilities;

3.3.2 is adequately resourced in terms of budget, tools and staff;

3.3.3 is continuously and adequately trained;

3.3.4 promotes a sound operational risk management culture across the organisation; and

3.3.5 communicates with the other lines of defence to reinforce the ORMF.

3.4 The seamless collaboration between these lines of defence can form a formidable shield, safeguarding not only individual REs but the entire financial system against potential threats and vulnerabilities.

4. 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 behaviour, and ensure that staff receives appropriate risk management and ethics training.

4.1 REs with a strong culture of risk management and ethical business practices are less likely to experience damaging Operational Risk events and are better placed to effectively deal with those events that occur. The actions of the Board of Directors and Senior Management as well as the RE's risk management policies, processes and systems provide the foundation for a sound risk management culture.

4.2 The Board of Directors should establish a code of conduct or an ethics policy to address conduct risk. This code or policy should be applicable to both staff and Board members. It should set clear expectations for integrity and ethical values of the highest standard, identify acceptable business practices, and prohibit conflicts of interest or the inappropriate provision of financial services (whether wilful or

negligent). It should be regularly reviewed and approved by the Board of Directors and attested by employees. Its implementation should be overseen by a senior ethics committee, or another Board-level committee, and should be publicly available (e.g., on the RE's website, branch premises). A separate code of conduct may be established for specific positions in the RE (e.g., treasury dealers etc.).

4.3 Senior Management should set clear expectations and define accountabilities to ensure RE's staff understand their roles and responsibilities of risk management, as well as their authority to act.

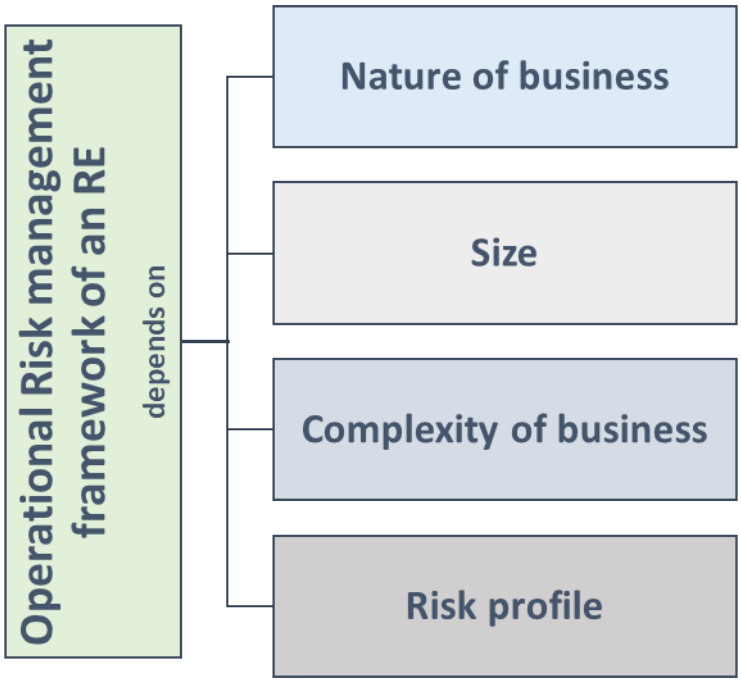
4.4 Compensation policies should be aligned to the RE's statement of risk appetite and tolerance as well as overall soundness of risk management framework, and appropriately balance risk and reward. Inappropriate incentives may result in increased litigation, reputational risk, or other risks to the RE. Therefore, the RE should review whether its existing governance and controls are adequate in light of risks arising from incentive arrangements.

4.5 Senior Management should ensure that an appropriate level of Operational Risk training is available at all levels throughout the organisation, such as heads of business units, heads of internal controls and senior managers. Training provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended. It should also appropriately include ethics training.

4.6 Strong and consistent support of the Board of Directors and Senior Management for operational risk management coupled with ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, etc.

Principle 2- 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 utilize 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 in order to minimise their impact on delivering critical operations through disruption.

4.7 The Board of Directors and Senior Management of RE should understand the nature and complexity of the risks inherent in the portfolio of RE's new business initiatives, products, services, activities, processes, and systems, which is a fundamental premise of sound risk management. This is particularly important for Operational Risk, as it is inherent in all business products, services, activities, processes, and systems.



4.8 The components of the ORMF should be fully integrated into the overall risk management processes of the RE by the first line of defence, adequately challenged and reviewed by the second line of defence, and independently reviewed by the third line of defence. The ORMF should be embedded across all levels of the RE

including group and business units as well as new business initiatives, products, services, activities, processes, and systems. In addition, results of the RE's Operational Risk assessment should be incorporated into the RE's overall business strategy development process. The overall approach to ORMF should reflect the following:

4.8.1 Management of Operational Risk is embedded within business lines of an RE.

4.8.2 Senior managers are responsible for management and ownership of Operational Risk across RE's end-to-end processes.

4.8.3 Board is ultimately responsible and accountable for oversight of Operational Risk Management.

4.9 The ORMF should be comprehensively and appropriately documented in Board of Directors approved policies and include definitions of Operational Risk and operational loss. If REs do not adequately describe and classify Operational Risk and loss exposure, it would result in significantly reducing the effectiveness of their ORMF.

4.10 ORMF documentation should clearly:

4.10.1 identify the governance structures used to manage Operational Risk, including reporting lines and accountabilities, and the mandates and membership of the Operational Risk governance committees;

4.10.2 reference the relevant Operational Risk Management policies and procedures;

4.10.3 describe the tools for risk and control identification and assessment and the role and responsibilities of the three lines of defence in using them;

4.10.4 describe the RE's accepted Operational Risk appetite and tolerance; the thresholds, material activity triggers or limits for inherent and residual risk; and the approved risk mitigation strategies and instruments;

4.10.5 describe the RE's approach to ensure controls are designed, implemented and operate effectively;

4.10.6 describe the RE's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

4.10.7 describe inventory risks and controls implemented by all business units (e.g., in a control library);

4.10.8 establish risk reporting and management information systems (MIS) for producing timely, and accurate data;

4.10.9 provide for a common taxonomy of Operational Risk terms to ensure consistency of risk identification, exposure rating and risk management objectives across all business units. The taxonomy can distinguish Operational Risk exposures by event types, causes, materiality and business units where they occur; it can also flag those operational risk exposures that partially or entirely represent legal, conduct, model and ICT (including cyber) risks as well as exposures in the credit or market risk boundary;

4.10.10 provide for appropriate independent review and challenge of the outcomes of the risk management process; and

4.10.11 require the policies to be reviewed and revised as appropriate based on continued assessment of the quality of the control environment addressing internal and external environmental changes or whenever a material change in the Operational Risk profile of the RE occurs.

5. 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 the ORMF and Operational Resilience approach effectively at all decision levels.

5.1 The Board of Directors should:

5.1.1 establish a risk management culture and ensure that the RE has adequate processes for understanding the nature and scope of the Operational Risk inherent in its current and planned strategies and activities;

5.1.2 ensure that the Operational Risk Management processes are subject to comprehensive and dynamic oversight and are fully integrated into, or coordinated with, the overall framework for managing all risks across the enterprise;

5.1.3 provide senior management with clear guidance regarding the principles underlying the ORMF, and approve the corresponding policies developed by senior management to align with these principles;

5.1.4 regularly review and evaluate the effectiveness of, and approve the ORMF to ensure the RE has identified and is managing the Operational Risk arising from external market changes and other environmental factors, as well as those Operational Risks associated with new products, services, activities, processes or systems, including changes in risk profiles and priorities (e.g. changing business volumes);

5.1.5 ensure that the RE's ORMF is subject to effective independent review by a third line of defence (audit or other appropriately trained independent third parties from external sources); and

5.1.6 ensure that, as best practices evolve, management is availing themselves of these advances.

5.2 Strong internal controls are a critical aspect of Operational Risk Management. The Board of Directors should establish clear lines of management responsibility and accountability for implementing a strong control environment. Controls should be regularly reviewed, monitored, and tested to ensure its ongoing effectiveness. The control environment should provide appropriate independence/separation of duties between Operational Risk Management functions, business units and support functions.

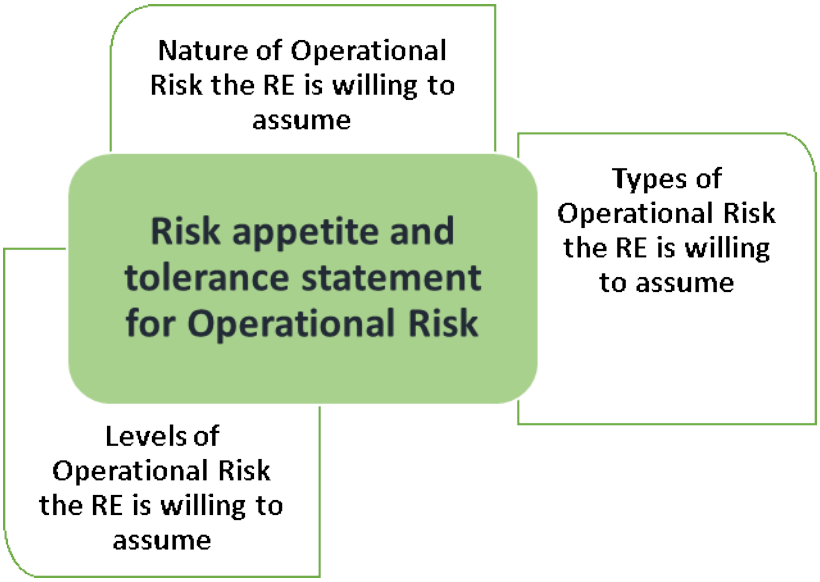
5.3 The Board of Directors should review and approve the RE's Operational Resilience approach considering the RE's risk appetite and tolerance for disruption to its critical operations. In formulating the RE's tolerance for disruption, the Board of Directors should consider its operational capabilities given a broad range of severe but plausible scenarios that would affect its critical operations. The Board of Directors should ensure that the RE's policies effectively address instances where the RE's capabilities are insufficient to meet its stated tolerance for disruption.

5.4 The Board of Directors should take an active role in establishing a broad understanding of the RE's operational resilience approach, through clear communication of its objectives to all relevant parties, including the RE's personnel, third parties, and intragroup entities.

5.5 Under the oversight of the Board of Directors, Senior Management should implement the RE's operational resilience approach and ensure that financial,

technical, and other resources are appropriately allocated in order to support the RE's overall operational resilience approach.

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, in order to enhance RE's Operational Resilience.



5.6 The risk appetite and tolerance statement for Operational Risk should be developed under the authority of the Board of Directors and linked to the RE's short and long-term strategic and financial plans. Taking into account the interests of the RE's customers and stakeholders as well as regulatory requirements, an effective risk appetite and tolerance statement should:

5.6.1 be easy to communicate and easy to understand for all stakeholders;

5.6.2 include key background information and assumptions that informed the RE's business plans at the time of its approval;

5.6.3 include statements that clearly articulate the motivation(s) for taking on or avoiding certain types of risk, and establish boundaries or indicators (which may be quantitative or not) to enable monitoring of these risks;

5.6.4 ensure that the strategy and risk limits of business units and legal entities, as relevant, align with the RE-wide risk appetite statement; and

5.6.5 be forward-looking and, where applicable, subject to scenario and stress testing to ensure that the RE understands what events might push it outside its risk appetite and tolerance statement.

5.7 The starting point for an RE in enhancing its operational resilience is to set the criteria for defining its critical operations. The Board of Directors should approve clearly defined and documented criteria to determine how operations are classified as critical. The criteria should enable an RE to identify its critical operations and prioritise them in the event of a disruption. This should be achieved by considering the risk a disruption poses to its customers, the RE's viability, safety and soundness, and overall financial stability. The criteria for the identification of critical operations should be reviewed and approved by the Board annually or at the time of implementing material changes to the business that would involve additional critical operations.

5.8 The Board of Directors should review and approve impact tolerances for each critical operation at least annually or as and when a disruption occurs. The purpose of impact tolerance is to quantify the maximum acceptable level of disruption for each critical operation. It needs to be tested against severe but plausible scenarios to determine their appropriateness, i.e., to determine whether the RE is able to stay within the defined impact tolerances during a disruption.

5.9 An RE should set at least one impact tolerance metric for each of its critical operations. At a minimum, there should be a (a) time-based metric (e.g., maximum acceptable duration a critical operation can withstand a disruption), (b) quantity-based metric (e.g., maximum extent of data loss that an RE would accept as a result of disruption) and (c) service level metric (e.g., minimum level of service that an RE would maintain while operating under alternative arrangements.) To further enhance its operational resilience, an RE should consider having additional impact tolerance metrics such as the maximum tolerable number of customers affected by a disruption; maximum number of transactions affected by a disruption; and the maximum value of transactions impacted.

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 of the RE's material products, activities, processes and systems consistent with its risk appetite and tolerance statement.

5.10 Senior Management should translate the ORMF approved by the Board of Directors into specific policies and procedures that can be implemented and verified within the different business units. It should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure the necessary resources are available to manage Operational Risk in line with the RE's risk appetite and tolerance statement. Moreover, it should also ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.

5.11 Senior Management is responsible for establishing and maintaining robust challenge mechanisms and effective issue resolution processes. These should include systems to report, track, and when necessary, escalate issues to ensure resolution. REs should be able to demonstrate that the three-lines-of-defence approach is operating satisfactorily and to explain how the Board of Directors, independent Audit Committee of the Board, and Senior Management ensure that this approach is implemented and operating in an appropriate manner.

5.12 Senior Management should ensure that staff responsible for managing Operational Risk co-ordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the RE who are responsible for the procurement of external services such as insurance risk transfer and other third-party arrangements. Failure to do so could result in significant gaps or overlaps in an RE's overall risk management programme.

5.13 The managers of the OORF within the RE should be of sufficient stature to perform their duties effectively, ideally evidenced by a title that is commensurate with other risk management functions such as credit, market and liquidity risk.

5.14 Senior Management should ensure that RE's activities are conducted by staff with the necessary experience, technical capabilities and access to resources. The

staff responsible for monitoring and enforcing compliance with the RE's risk policy should have authority independent from the units they oversee.

5.15 An RE's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the Operational Risk governance structure, an RE should take the following into consideration:

5.15.1 Committee structure – A sound industry practice for larger and more complex organisations with a central group function and separate business units to utilise a Board-created enterprise-level risk committee for overseeing all risks, to which a management level Operational Risk Committee reports. Depending on the nature, size and complexity of the RE, the enterprise-level risk committee may receive input from Operational Risk committee(s), business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees Operational Risk directly within the Board's risk management committee.

5.15.2 Committee composition – A sound industry practice for Operational Risk committees (or the risk committee in smaller REs) is to include members with a variety of expertise, which should cover expertise in business activities, financial activities, legal, technological and regulatory matters, and risk management.

5.15.3 Committee operation – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate and documented to permit review and evaluation of committee effectiveness.

5.16 Because Operational Risk Management is an evolving area, and the business environment is constantly changing, Senior Management should ensure that the RE's policies, processes and systems under ORMF remain sufficiently robust to manage and ensure that operational losses are adequately addressed in a timely manner. Improvements in Operational Risk Management depend heavily on senior management's willingness to be proactive and also act promptly and appropriately to address Operational Risk managers' concerns.

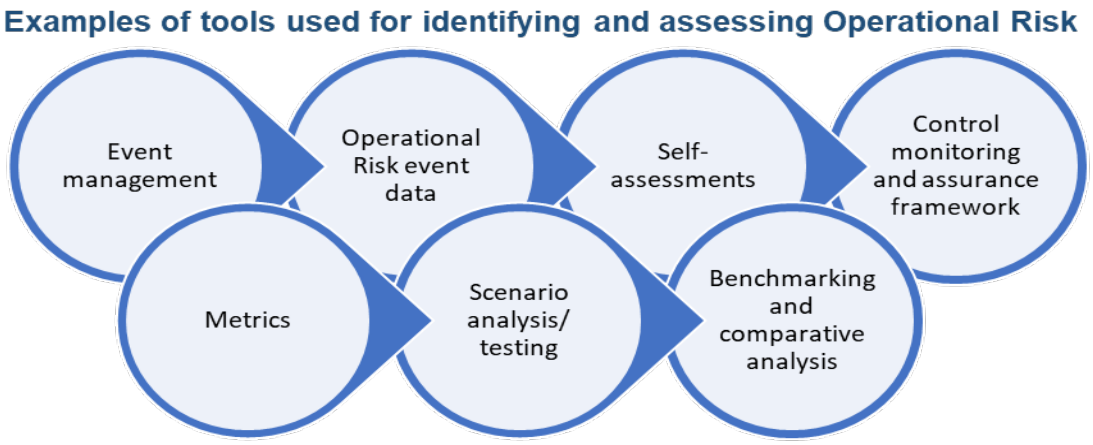
6. Risk management environment - Identification and assessment

Principle 6: Senior Management should ensure the comprehensive identification and assessment of the Operational Risk inherent in all material products, activities, processes and systems to make sure 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 in a proactive and prompt manner. All the resulting risks should be managed in accordance with operational resilience approach.

6.1 Risk identification and assessment are fundamental characteristics of an effective Operational Risk Management system, and directly contribute to operational resilience capabilities. Effective risk identification considers both internal and external factors. Sound risk assessment allows an RE to better understand its risk profile and allocate risk management resources and strategies most effectively.

For example, figure below shows the wide spectrum of risks (risk universe) which could be existing in third-party relationships.

6.2 Examples of tools (indicative and not exhaustive) used for identifying and assessing Operational Risk are:



6.2.1 Self-assessments – REs often perform self-assessments of their Operational Risks and controls at various levels. The assessments typically evaluate inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered) and contain both quantitative (such as metrics, benchmarking, etc.) and qualitative (such as likelihood and consequence of the risk event in determination of inherent and residual risk ratings) elements. The assessments may utilise business process mapping to identify key steps in business processes, activities, and organisational functions, as well as the associated risks and areas of control weakness. The assessments should contain sufficiently detailed information on the business environment, Operational Risks, underlying causes, controls and evaluation of control effectiveness to enable an independent reviewer to determine how the RE reached its ratings. A risk register can be maintained to collate this information to form a meaningful view of the overall effectiveness of controls and facilitate oversight by senior management, risk committees, and the Board of Directors.

6.2.2 Operational Risk event data – REs often maintain a comprehensive Operational Risk event dataset that collects all material events experienced by the RE and serves as basis for Operational Risk assessments. The event dataset typically includes internal loss data, near misses, etc., and is classified according to a taxonomy defined in the ORMF policies and consistently applied across the RE. It also includes the date of the event (occurrence date, discovery date and accounting date) and, in the case of loss events, financial impact. When other root cause information for events is available, ideally it can also be included in the Operational

Risk dataset. Where feasible, REs are encouraged to also seek to gather external Operational Risk event data and use this data in their internal analysis, as it is often informative of risks that are common across the industry.

6.2.3 Event management – A sound event management approach typically includes analysis of events to identify new Operational Risks, understanding the underlying causes and control weaknesses, and formulating an appropriate response to prevent recurrence of similar events. This information is an input to the self-assessment and, in particular, to the assessment of control effectiveness.

6.2.4 Control monitoring and assurance framework – Incorporating an appropriate control monitoring and assurance framework facilitates a structured approach to the evaluation, review and ongoing monitoring and testing of key controls. The analysis of controls ensures these are suitably designed for the identified risks and are operating effectively. The analysis should also consider the sufficiency of control coverage, including adequate prevention, detection and response strategies. The control monitoring and testing should be appropriate for the different Operational Risks and across business areas. Further details on control and mitigation are given in paragraph 9 of this Guidance Note.

6.2.5 Metrics – Using Operational Risk event data and risk and control assessments, REs often develop metrics to assess and monitor their Operational Risk exposure. These metrics may be simple indicators, such as event counts, or result from more sophisticated exposure models. Metrics provide early warning information to monitor ongoing performance of the business and the control environment, and to report the Operational Risk profile. Effective metrics clearly link the associated Operational Risks and controls. Monitoring metrics and related trends through time against laid down thresholds or limits or tolerance levels provides valuable information for risk management and reporting purposes.

6.2.6 Scenario analysis – Scenario analysis is a method to identify, measure and analyse a range of scenarios, including low probability and high severity events, some of which could result in severe Operational Risk losses. It typically involves workshops or meetings of subject matter experts including senior management, business management and senior Operational Risk staff and other functional areas such as compliance, human resources and IT risk management, to develop and analyse the drivers and range of consequences of potential events. Inputs to the

scenario analysis would typically include relevant 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. The scenario analysis process could be used to develop a range of consequences of potential events, including impact assessments for risk management purposes, supplementing other tools based on historical data or current risk assessments. An RE must carry out regular scenario analysis using the above parameters, for testing its ability to remain within its impact tolerance in the event disruption of its operations, for each of its critical services. In carrying out the scenario analysis, an RE must identify the range of adverse circumstances of varying nature, severity and duration, relevant to its business and risk profile and consider the risks to delivery of the RE's critical services in those circumstances. Such an exercise could also be integrated with disaster recovery and business continuity plans, for further testing of operational resilience. Given the subjectivity of the scenario process, a robust governance framework and independent review are important to ensure the integrity and consistency of the process.

6.2.7 Benchmarking and comparative analysis – Benchmarking and comparative analysis are comparisons of the outcomes of different risk measurement and management tools deployed within the RE, as well as comparisons of metrics of the RE, with other REs in the industry. Such comparisons can be performed to enhance understanding of the RE's Operational Risk profile. For example, comparing the frequency and severity of internal losses with self-assessments can help the RE determine whether its self-assessment processes are functioning effectively. Scenario analysis data can be compared with internal and external loss data to gain a better understanding of the severity of the RE's exposure to potential risk events.

6.3 REs should ensure that the Operational Risk assessment tools' outputs are:

6.3.1 based on accurate data, whose integrity is ensured by strong governance and robust verification and validation procedures;

6.3.2 adequately taking into account the internal pricing and performance measurement mechanisms as well as business opportunities assessments; and

6.3.3 subject to OORF-monitored action plans or remediation plans when necessary.

6.4 These Operational Risk assessment tools directly contribute to an RE's operational resilience approach, in particular event management, self-assessment and scenario analysis procedures, as they allow REs to identify and monitor both internal and external threats and vulnerabilities to their critical operations. REs should use the outputs of these tools on a regular basis and in a timely manner to manage, address and improve their operational resilience controls and procedures so as to prevent them from affecting critical operations delivery. In doing so, the Operational Risk Management function should work alongside other relevant functions. These assessments should also be conducted in the event of changes to any underlying components of the critical operations, as well as after incidents in order to take into account lessons learned and new threats and vulnerabilities, if any, that caused the incident.

7. Change Management

Principle 7: Senior Management should ensure that the RE's change management process is comprehensive, appropriately resourced and adequately articulated between the relevant lines of defence.

7.1 In general, an RE's Operational Risk exposure evolves when an RE initiates change, such as engaging in new activities or developing new products or services; entering into unfamiliar markets or jurisdictions; implementing new or modifying business processes or technology systems; and/or engaging in businesses that are geographically distant from the Head Office. Change management should assess the evolution of associated risks across time, from inception to termination (e.g. throughout the full life cycle of a product[8]).

7.2 An RE should have policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change on the basis of agreed objective criteria. Change implementation should be monitored by specific oversight controls. Change management policies and procedures should be subject to independent and regular review and update, and clearly allocate roles and responsibilities in accordance with the three-lines-of-defence model, in particular:

7.2.1 The first line of defence should perform Operational Risk and control assessments of new products, services, activities, processes and systems, including the identification and evaluation of the required change through the decision-making

[8] The life cycle of a product or service encompasses various stages from the development, ongoing changes, grandfathering and closure. Indeed, the level of risk may escalate for example when new products, services, activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations.

and planning phases to the implementation of the change and post-implementation review.

7.2.2 The second line of defence (OORF) should challenge the Operational Risk and control assessments of first line of defence, as well as monitor the implementation of appropriate controls or remediation actions. OORF should cover all phases of this process. In addition, OORF should ensure that all relevant control groups (e.g., finance, compliance, legal, business, ICT, risk management) are involved as appropriate.

7.2.3 The third line of defence may review the above as per the mandate defined at paragraph 3.2.3.

7.3 As a part of the change management exercise, an RE should have policies and procedures for the review and approval of new products, services, activities, processes, and systems. The review and approval process should consider:

7.3.1 Inherent risks – including legal, ICT, and model risks – in the launch of new products, services, activities, and operations in unfamiliar markets, and in the implementation of new processes, people and systems (especially when third party services are used).

7.3.2 Changes to the RE's Operational Risk profile, appetite and tolerance, including changes to the risk of existing products or activities, especially critical operations.

7.3.3 The necessary controls, risk management processes, and risk mitigation strategies.

7.3.4 The residual risk.

7.3.5 Changes to relevant risk thresholds or limits.

7.3.6 The procedures and metrics to assess, monitor, and manage the risk of new products, services, activities, markets, jurisdictions, processes and systems.

7.4 The review and approval process should include ensuring that appropriate investment has been made for human resources and technology infrastructure before changes are introduced. Changes should be monitored, during and after their implementation, to identify any material differences to the expected Operational Risk profile and manage any unexpected risks.

7.5 REs should maintain a central record of their products and services to the extent possible (including the third-party arrangements) to facilitate the monitoring of changes.

7.6 REs should leverage change management capabilities in accordance with the change management processes as a way to assess potential effects on the delivery of critical operations and their interconnections and interdependencies for ensuring operational resilience.

8. 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.

8.1 An RE should ensure that its reports are comprehensive, accurate, consistent and actionable across business units and products. To this end, the first line of defence should ensure reporting on any residual Operational Risks, including Operational Risk events, control deficiencies, process inadequacies, and non-compliance with Operational Risk tolerances. Reports should be manageable in scope and volume by providing an outlook on the RE's Operational Risk profile and adherence to the Operational Risk appetite and tolerance statement; effective decision-making is impeded by both excessive amounts and paucity of data.

8.2 Reporting by RE should be timely and should be able to produce reports in both normal and stressed market conditions.[9] The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. 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 and/or risk management functions. Reports generated by or for supervisory authorities should also be reported internally to Senior Management and the Board of Directors.

8.3 Operational Risk reports should describe the Operational Risk profile of the RE by providing internal financial, operational, and compliance indicators, as well as

[9] Reporting should be consistent with BCBS' Principles for effective risk data aggregation and risk reporting (https://www.bis.org/publ/bcbs239.pdf).

external market or environmental information about events and conditions that are relevant to decision making.

Operational Risk reports should include:	Breaches of the RE's risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements.
	A discussion and assessment of key and emerging risks.
	Details of recent significant internal Operational Risk events and losses (including root cause analysis).
	Identification of near misses and an assessment of efficacy of controls.
	Relevant external events or regulatory changes and any potential impact on the RE

8.4 Data capture and risk reporting processes should be analysed periodically with the goal of enhancing risk management performance as well as advancing risk management policies, procedures and practices.

8.5 Further, Senior Management should provide timely reports to the Board on the ongoing operational resilience of the RE's business units to support the Board's oversight, particularly when significant deficiencies could affect the delivery of the RE's critical operations.

9. 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.

9.1 Internal controls should be designed to provide reasonable assurance that an RE will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme consists of four components that are integral to the risk management process: risk assessment, control activities, information and communication, and monitoring activities.[10]

[10] BCBS paper on "Framework for Internal Control Systems in Banking Organisations, September 1998" discusses internal controls in greater detail.

9.2 Control processes and procedures should include a system for ensuring compliance with policies, regulations and laws. Examples of principal elements of a policy compliance assessment are:

Examples of principal elements of a policy compliance assessment are:
• Top-level reviews of progress towards stated objectives
• Verification of compliance with management controls
• Review of the treatment and resolution of instances of non-compliance
• Evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management
• Tracking of reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy, regulations and laws

9.3 Controls processes and procedures should address how the RE ensures continuity of operations in both normal circumstances and in the event of disruption, reflecting respective functions' due diligence, consistent with the RE's operational resilience approach.

9.4 An effective control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team, without dual controls {e.g., a process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information} or other countermeasures, may result in concealment of losses, errors or other inappropriate actions. Therefore, areas where conflicts of interest may arise should be identified, minimised, and be subject to careful monitoring and review.

9.5 In addition to segregation of duties and dual controls, REs should ensure that other traditional internal controls are in place, as appropriate, to address Operational Risk. Some of the examples of these controls are given in table below:

Examples of these controls are:
• Clearly established authorities and/or processes for approval
• Close monitoring of adherence to assigned risk thresholds or limits
• Safeguards for access to, and use of, RE assets and records
• Appropriateness of staffing level and training to maintain technical expertise
• Ongoing processes to identify business units or products where returns appear to be out of line with reasonable expectations.
• Regular verification and reconciliation of transactions and accounts
• Mandatory leave policy that allows for employees posted in sensitive positions or areas of operations to compulsorily be sent on leave for a stipulated period in a single spell every year, while maintaining an element of surprise for the employee.

9.6 Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that should be addressed through sound technology governance and infrastructure risk management programmes.

9.7 The use of technology related products, services, activities, processes and delivery channels exposes an RE to Operational Risk and the possibility of material financial loss. Consequently, an RE should have an integrated approach to identifying, measuring, monitoring and managing technology risks along the same precepts as Operational Risk Management. (Also refer to paragraph 15 of this Guidance Note)

9.8 While recourse to entities such as, but not limited to third-party service providers can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that RE should address. The integrated approach adopted by RE for its ORMF should necessarily include such third-party dependencies. Amongst others, the concentration of risk, complexity and downstream dependencies with regard to third-party service providers should be taken into account. While these risks may be unavoidable, identifying and monitoring of such risks would allow REs to initiate actions that could reasonably mitigate or manage them. These risk policies and risk management activities should include

critical operations management and dependency management. (Also refer to paragraph 12 of this Guidance Note)

9.9 In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management may complement controls by seeking to transfer the risk to another party such as through insurance. The Board of Directors should determine the maximum loss exposure the RE is willing to take and has the financial capacity to assume and should perform an annual review of the RE's risk and insurance management programme, including specific insurance or risk transfer needs of an RE.

9.10 Because risk transfer is an imperfect substitute for sound controls and risk management programmes, REs should view risk transfer tools as complementary to, rather than a replacement for internal Operational Risk controls. Having mechanisms in place to quickly identify, recognise and rectify distinct Operational Risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (e.g., counterparty risk, legal risk).

Pillar 2: Build Resilience

10 Essential Elements of Operational Resilience

10.1 Operational resilience is an outcome that benefits from the effective management of Operational Risk. Activities such as risk identification and assessment, risk mitigation (including the implementation of controls) and the monitoring of risks and control effectiveness work together to minimise operational disruptions and their effects. The overarching principle of operational resilience is the acceptance that disruptions will occur, and that REs need to be prepared to respond accordingly and have measures in place to limit the impact. The REs need to ensure that they have prepared effectively, and have the flexibility to withstand, absorb, respond, adapt and recover and learn from disruptions with minimal impact on their critical operations. Further, management’s focus on the RE’s ability to respond to and recover from disruptions, assuming failures will occur, will support operational resilience. An operationally resilient RE is less prone to incur untimely lapses in its operations and losses from disruptions, thus lessening impact on critical operations

and related services, functions and systems. While it may not be possible to avoid certain Operational Risks, such as a pandemic, it is possible to improve the resilience of an RE's operations to such events.

10.2 Business continuity, dependencies on third parties, and the technology upon which REs rely are important factors for REs to consider when strengthening their operational resilience.

10.3 It is essential for REs to ensure that existing risk management frameworks, business continuity plans, and third-party dependency management are implemented consistently within the organisation. As operational resilience draws from such elements like business continuity, third-party risk management, ICT & cyber risk management, incident management, and wider aspects of Operational Risk Management, a holistic approach is essential if an RE is to enhance the resilience of its critical operations, regardless of the type of disruption. Approaching operational resilience through a critical operations lens encourages an RE to prioritise what is critical or important to the RE and the financial system, and understand the interconnections and interdependencies involved in delivering those operations. REs should therefore verify that their operational resilience approach is appropriately harmonised with the stated actions, organisational mappings, critical operations and critical shared services (including the services which are essential for the industry) contained in their recovery and resolution plans, which ultimately are important for the financial system stability.

11. 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.

11.1 The respective functions should map (i.e., identify and document) the people, technology, processes, information, facilities, and the interconnections and interdependencies among them as needed to deliver the RE's critical operations, including those dependent upon, but not limited to, third parties or intragroup arrangements.

11.2 REs may leverage their recovery and resolution plans, as appropriate, for definitions of critical operations and should consider whether their operational

resilience approaches are appropriately harmonised with those of the organisational mappings of critical operations and critical third-party service providers as contained in their respective recovery and resolution plans.

11.3 The approach and level of granularity of mapping should be sufficient for REs to identify vulnerabilities and to support testing of their ability to deliver critical operations through disruption, considering the RE's risk appetite and tolerance for disruption. Such a mapping will enable the RE to pinpoint vulnerabilities in how critical operations are being delivered and determine where recovery and resolution plans can be leveraged. Examples of such vulnerabilities could include concentration risk, single points of failure, and inadequate substitutability of service providers and resources.

11.4 Where an RE is a member of a group, it must ensure that any additional risks arising elsewhere in the group are accounted for that may affect its ability to tackle with a severe but plausible disruption to its operations.

12. 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.

12.1 REs should perform a risk assessment and due diligence before entering into arrangements including those of, but not limited to, third parties (which include intragroup entities), consistent with its ORMF,[11] third-party risk management policy, and operational resilience approach. Prior to entering into such an arrangement, the RE should verify whether the third party, including, the intragroup entity to these arrangements, has at least an equivalent level of operational resilience to safeguard the RE's critical operations in both normal circumstances and the event of a disruption.

[11] The management of dependencies articulated in this principle should be consistent with and conducted alongside the control and risk mitigation policies (principle 9) of this Guidance Note.

Few examples of what constitute third-party service providers is shown in figure below (indicative and not an exhaustive list)

12.2 The Board of Directors and Senior Management are responsible for understanding the Operational Risks associated with third-party arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in such activities. A Board approved policy on management of service providers is critical for managing risks associated with reliance on third parties whether related or unrelated to RE. Third-party risk policies (as a part of the ORMF's policies) and risk management activities should encompass:

12.2.1 Procedures for determining whether there is a need for entering into a third-party arrangement for a service and how to enter into such an arrangement.

12.2.2 Processes for conducting due diligence in the selection of potential service providers.

12.2.3 Sound structuring of the third-party arrangement, including ownership and confidentiality of data, as well as termination rights.

12.2.4 Programmes for managing and monitoring the risks associated with the third-party arrangement, including the financial condition of the service provider.

12.2.5 Establishment of an effective control environment at the RE and the service provider that should include a register of third-party relationships (that identifies the criticality of different services) and metrics and reporting to facilitate oversight of the service provider.

12.2.6 Development of viable contingency plans.

12.2.7 Execution of comprehensive contracts and/or service level agreements (which are enforceable) with a clear allocation of responsibilities between the third-party service provider and the RE, provided the ultimate responsibility vests with the RE.

12.2.8 REs' supervisory and resolution authorities' access to third parties.

12.3 REs should develop appropriate business continuity including contingency planning procedures and exit strategies to maintain their operational resilience in the event of a failure or disruption at a third-party level impacting the provision of critical operations. Scenarios under the RE's business continuity plans should assess the substitutability of third parties that provide services to the RE's critical operations, and other viable alternatives that may facilitate operational resilience in the event of an outage at a third party, such as bringing the service back in-house.

12.4 Along with an increasing reliance on service providers, complexity in supply chains have also risen. A large number of service providers are subcontracting the services who are themselves reliant on another service provider for the provision of a service (a fourth party). In certain cases, these fourth party service providers can, in turn, be reliant upon yet another service provider, and further till nth service provider, thus elongating the chain. Such an arrangement results in an RE relying on downstream service providers without a direct agreement in place. Such supply chain vulnerabilities and lack of transparency may increase Operational Risk for RE. This can also impede its ability to manage risks in the supply chain as well have an effect on the regulator's expectations on the RE. Therefore, REs are expected to be aware of, and manage, the risks associated with any further downstream service providers, to maintain a thorough understanding of the supply chain and potential issues that could affect the entity's ability to maintain its critical operations. Therefore, REs, in their agreement with the service providers, should include clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors (including nth parties in the supply chain).

13. 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.

13.1 Sound and effective governance of REs' business continuity plan requires:

13.1.1 Regular review and approval by the Board of Directors.

13.1.2 The strong involvement of the Senior Management and business units' leaders in its implementation.

13.1.3 The commitment of the first and second lines of defence to its design.

13.1.4 Regular review by the third line of defence.

13.2 REs should prepare forward-looking business continuity plan (BCP) with scenario analyses associated with relevant impact assessments and recovery procedures:

13.2.1 An RE should ground its business continuity plan on scenario analyses of potential disruptions that identify and categorise critical business operations and key internal or external dependencies. In doing so, REs should cover all their business units as well as critical providers and major third parties.

13.2.2 Each scenario should be subject to a quantitative and qualitative impact assessment or business impact analysis (BIA) with regards to its financial, operational, legal and reputational consequences.

13.2.3 Disruption scenarios should be subject to thresholds or limits (such as maximum tolerable outage) for the activation of a business continuity procedure. The business continuity procedure should meet the defined recovery time objectives (RTO) and recovery point objectives (RPO). The procedure should also address recovery strategies and methodologies, resumption aspects, as well as communication guidelines for informing management, employees, regulatory authorities, customers, suppliers, and where appropriate other authorities.

13.2.4 These plans should also incorporate testing programmes, training and awareness programmes, and communication and crisis management programmes.

13.3 Business continuity plans should develop, implement and maintain a regular business continuity exercise encompassing critical operations and their interconnections and interdependencies, including those through relationships with, but not limited to, third parties and intragroup entities. Business continuity exercises should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents. Among other business continuity goals, business continuity exercises should support staff's operational resilience awareness including training of staff which should be customised based on specific cases so that they can effectively adapt and respond to incidents.

13.4 Business continuity plans should provide detailed guidance for implementing the RE's disaster recovery framework. These plans should establish the roles and responsibilities for managing operational disruptions and provide clear guidance regarding the succession of authority in the event of a disruption that impacts key personnel. Additionally, these plans should clearly set out the internal decision-making process and define the triggers for invoking the RE's business continuity plan.

13.5 REs' business continuity plans for the delivery of critical operations and critical third-party services contained in their recovery and resolution plans should be consistent with their operational resilience approaches.

13.6 An RE should periodically review its business continuity plans and policies to ensure that strategies remain consistent with current operations, risks and threats. Business continuity procedures should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, an RE should participate in business continuity testing with service providers. Results of formal testing and review activities should be reported to Senior Management and the Board of Directors.

13.7 In view of Covid-19, preparing for future pandemics of varied kind should be one of REs' top priorities. One key challenge REs face in such pandemics is the possibility of low staff availability which could potentially disrupt business operations for prolonged periods. The Business Continuity Planning of an RE should therefore include measures to mitigate the impact of such future pandemics. REs should put in place a comprehensive organisation-wide preparedness and response plan to deal with the different stages of a future outbreak or any such unforeseeable

circumstances. The plan should preferably be aligned with the comprehensive ORMF of the RE.

14. 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 the lessons learned from previous incidents.

14.1 REs should maintain an inventory of incident response and recovery, internal and third-party resources to support its response and recovery capabilities.

14.2 The scope of incident management should capture the life cycle of an incident,[12] typically including, but not limited to:

14.2.1 The classification of an incident's severity based on predefined criteria (e.g., expected time to return to business as usual), enabling proper prioritisation of and assignment of resources to respond to an incident.

14.2.2 The incident response and recovery procedures, including their connection to the RE's business continuity, disaster recovery, and other associated management plans and procedures.

14.2.3 The implementation of communication plans to report incidents to both internal and external stakeholders (e.g., regulatory authorities), including performance metrics during, and analysis of lessons learned after an incident. The internal communication plan should contain escalation routes on how to communicate with key decision makers, operational staff and third parties, if necessary. The external communication plan should outline how the entity will communicate with its customers, stakeholders, and regulators during a disruption.

14.3 Incident response and recovery procedures should be periodically reviewed, tested, and updated by the REs. They should also identify and address the root causes of incidents to prevent or minimise serial recurrence.

14.4 The lessons learned from previous incidents including incidents experienced by others as well as near misses should be duly reflected when updating the incident management programme. An RE's incident management programme should

[12] Recognising that the life cycle of an incident could span multiple measures of time that could range from hours to weeks to months.

manage all incidents impacting the RE, including those attributable to dependencies on, but not limited to, third parties and intragroup entities.

15. 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.

15.1 Effective ICT performance and security are paramount for an RE to conduct its business properly. The appropriate use and implementation of sound ICT risk management contributes to the effectiveness of the control environment and is fundamental to the achievement of an RE's strategic objectives. An RE's ICT risk assessment should ensure that its ICT fully supports and facilitates its operations. ICT risk management should reduce an RE's Operational Risk exposure to direct losses, legal claims, reputational damage, ICT disruption and misuse of technology in alignment with its risk appetite and tolerance statement.

15.2 ICT risk management includes:

15.2.1 ICT risk identification and assessment, including critical information, assets and infrastructure.

15.2.2 ICT risk mitigation measures consistent with the assessed risk level (e.g. cybersecurity, response and recovery programmes, ICT change management processes, ICT incident management processes, including relevant information transmission to users on a timely basis).

15.2.3 Monitoring of these mitigation measures (including regular tests).

15.3 REs should have a documented ICT policy, including cyber security, which stipulates governance and oversight requirements, risk ownership and accountability, ICT security measures (e.g., access controls, critical information asset protection, identity management), periodic evaluation and monitoring of cyber security controls, and incident response, as well as business continuity and disaster recovery plans.

15.4 To ensure data and systems' confidentiality, integrity and availability, the Board of Directors/ its Committee should regularly oversee the effectiveness of the RE's ICT risk management and Senior Management should routinely evaluate the design, implementation and effectiveness of the RE's ICT risk management. This requires regular alignment of the business, risk management and ICT strategies to be consistent with the RE's risk appetite and tolerance statement as well as with privacy and other applicable laws. REs should continuously monitor its ICT and regularly report to Senior Management on ICT risks, controls and events.

15.5 ICT risk management together with complementing processes set by the REs should:

15.5.1 be reviewed on a regular basis for completeness against relevant industry standards and best practices as well as against evolving threats (e.g., cyber) and evolving or new technologies. Threat profile for critical information assets should be reviewed and tested for vulnerabilities on a more frequent basis in order to ensure resilience to the ICT related risks;

15.5.2 be regularly tested as part of a programme to identify gaps against stated risk tolerance objectives and facilitate improvement of the ICT risk identification/ detection and event management; and

15.5.3 make use of actionable intelligence to continuously enhance their situational awareness of vulnerabilities to ICT systems, networks and applications and facilitate effective decision making in risk or change management.

15.6 REs should develop approaches to ICT readiness for stressed scenarios from disruptive external events, such as the need to facilitate the implementation of wide-scale remote-access, rapid deployment of physical assets and/or significant expansion of bandwidth to support remote user connections and customer data protection. REs should ensure that:

15.6.1 appropriate risk mitigation strategies are developed for potential risks associated with a disruption or compromise of ICT systems, networks and applications. They should evaluate whether the risks, taken together with these strategies, fall within its risk appetite and risk tolerance;

15.6.2 well defined processes for the management of privileged users and application development are in place; and

15.6.3 regular updates are made to ICT including cyber security in order to maintain an appropriate security posture.

15.7 In light of the recent shift in preferences and the dependence on technology for functioning of REs, they should prioritise their cyber security efforts based on ICT risk assessment and the significance of the critical information assets for its critical operations while observing all pertinent legal and regulatory requirements relating to data protection and confidentiality. REs should develop plans and implement controls to maintain the integrity of critical information in the event of a cyber-event, such as secure storage and offline backup on immutable media of data supporting critical operations.

Pillar 3: Learn and Adapt

16. Disclosure and Reporting

Principle 15: An RE's public disclosures should allow stakeholders to assess its approach to Operational Risk management and its Operational Risk exposure.

16.1 An RE's public disclosure of relevant Operational Risk Management information can lead to transparency and the development of better industry practices through market discipline. The disclosures also allow REs to undertake a peer-to-peer comparative analysis for improving their own processes and controls. The extent and type of disclosure should be commensurate with the size, risk profile and complexity of an RE's operations, and evolving industry practice.

16.2 REs should disclose relevant Operational Risk exposure information to their stakeholders (including significant operational loss events), while not creating Operational Risk through this disclosure (e.g., description of unaddressed control vulnerabilities). An RE should disclose its ORMF in a manner that allows stakeholders to determine whether the RE identifies, assesses, monitors and controls/mitigates Operational Risk effectively.

16.3 REs should have a formal disclosure policy that is subject to regular and independent review and approval by the Senior Management and the Board of Directors, respectively. The policy should address the RE's approach for determining what Operational Risk disclosures it will make and the internal controls over the

disclosure process. In addition, REs should implement a process for assessing the appropriateness of their disclosures and disclosure policy.

16.4 Where possible, direct reporting mechanisms with supervisors and auditors may be established for ensuring an ongoing review of the ORMF also enabling supervisors to encourage REs' ongoing internal development efforts by monitoring, comparing and evaluating REs' recent improvements and plans for prospective developments.

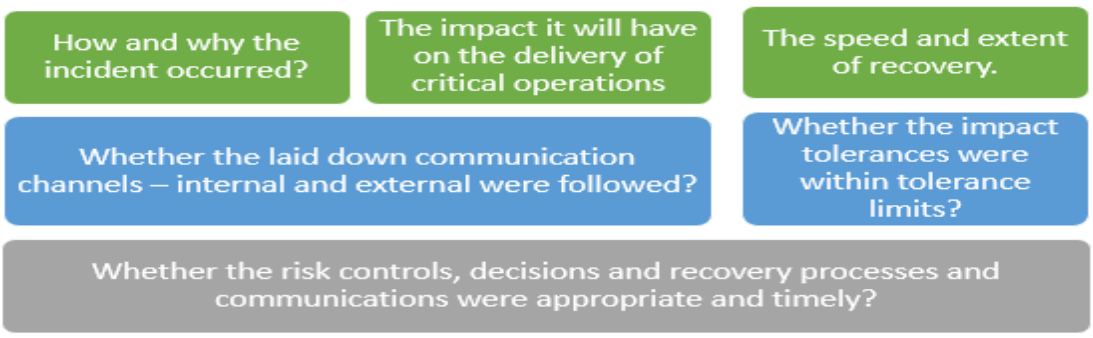
17. Lessons Learned Exercise and Adapting

Principle 16: A lessons learned exercise should be conducted after a disruption to a critical or important business service to enhance an RE's capabilities to adapt and respond to future operational events.

17.1 An RE should conduct a 'lessons learned exercise', including Root Cause Analysis, after any disruption to a business service with emphasis on critical service. This includes any potential material disruption to a third-party provider (including but not limited to a group entity) that feeds into the delivery of a critical business service.

17.2 The lessons learned exercise should utilise the information gathered as part of the incident management and disaster recovery process. The decisions and recovery processes determined to be appropriate throughout the incident management process should form the basis of the lessons learned exercise.

17.3 An RE should have predetermined criteria or questions basis the lessons learned exercise from the incidents. These questions should identify deficiencies, which caused induced failure in the continuity of service and these deficiencies should be addressed as a matter of priority. Specifically, at a minimum, the following should be considered:



17.4 The lessons learned exercises should define effective remediation measures to redress deficiencies and failure in the continuity of service. The more efficient use of resources for critical operations and adjustments to any impact tolerances determine whether a failure could have a wider impact on financial stability. A report/ self-assessment analysis document post the incident containing the above should be presented to the Board.

17.5 The lessons learned exercise allows an RE to reflect on the three-pillar approach to operational resilience and allows for a feedback loop into the first two pillars that encourages improvement in how an RE prepares for and recovers from disruptions. Doing so will also allow an RE to agree remedial actions and adjust any impact tolerances if determined.

18. 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.

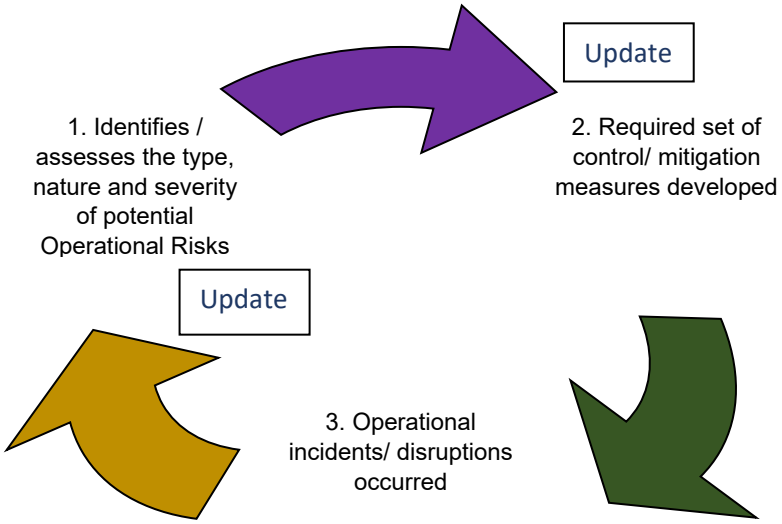
18.1 Continuous improvements to operational resilience requires an RE to learn from its experiences as changes to its operational approaches or technology infrastructure mature over time. This should not only occur after a disruption or incident has occurred but should form part of ongoing operational resilience discussions.

18.2 An RE should promote an effective culture of learning and continuous improvement as operational resilience evolves. Operational resilience needs to be a fundamental element of any strategic decision taken by an RE.

18.3 REs should develop robust feedback systems to ensure a continuous positive feedback loop fostering an effective learning environment, which in turn helps them frame better ORMFs and build adequate Operational Resilience.

18.4 In the above context, an effective feedback system properly identifies and assesses the type, nature and severity of potential Operational Risks that could be faced by an RE as well as where the vulnerabilities lie and need to be addressed. Based on the same, a required set of control and mitigation measures can be developed to tackle these risks. Further, based on real time operational incidents or disruptions that have occurred despite the mitigation measures, the feedback system

updates the type, nature and severity of potential Operational Risks and hence updates the required set of control and mitigation measures to tackle these risks. Errors/mistakes in the existing controls and processes should also be incorporated in the feedback for ensuring rectification and necessary updation. In this way, through feedback, an RE maintains optimal operational resilience as shown in figure below.



Annex

Key changes carried out in the Guidance Note vis-à-vis repealed Guidance Note

Particulars	Repealed Guidance Note dated October 14, 2005	Guidance Note
Focus	Operational risk management.	Operational resilience as an outcome of operational risk management.
Applicability	It is applicable to Scheduled Commercial Banks.	It is applicable to all Commercial Banks, all Non-Banking Financial Companies (NBFCs), all Co-operative Banks, and all All India Financial Institutions (AIFIs).
Three lines of defence model	It does not contain guidance on 'Three lines of defence' model.	It explicates the 'Three lines of defence model' wherein ▪ Business unit forms the first line of defence, ▪ Organizational operational risk management function (including compliance function) forms the second line of defence, and ▪ Audit function forms the third line of defence.
Typical organisational set up	It provides a typical organisational setup for operational risk management.	As now a variety of regulated entities (REs) are covered, for whom the organisational setup would vary based on the size and nature of activities, the typical organisational setup has not been specified.
Change	It has not explicitly	It has an updated guidance on

Particulars	Repealed Guidance Note dated October 14, 2005	Guidance Note
management	specified change management.	change management with a specifically detailed Principle on it.
Mapping of internal and external interconnections and interdependencies, Incident management, Information and communication technology (ICT), and Disclosures	It is silent on the mapping of internal and external interconnections and interdependencies, incident management, ICT, and disclosures.	It has separate Principles for mapping of internal and external interconnections and interdependencies, incident management, ICT, and disclosures.
Third-party relationships	It has scattered guidance on outsourcing.	It has a focused Principle on Third-party relationship, which is a broader concept than outsourcing.
Lessons learned and feedback	It has very limited/no guidance on lessons learnt exercise and continuous feedback mechanism.	It has introduced separate Principles on lessons learned exercise and continuous feedback mechanism.
Approaches for operational risk capital calculation	It has detailed approaches for operational risk capital calculation.	It has dropped the approaches for operational risk capital calculation as REs such as Local Area Banks, Small Finance Banks, Payments Banks, Regional Rural Banks, NBFCs, and Co-operative

Particulars	Repealed Guidance Note dated October 14, 2005	Guidance Note
		Banks, (covered under the Guidance Note) are presently not required to maintain a separate regulatory capital for operational risk. Further, the approach for operational risk capital calculation for banks (Public Sector Banks, Private Banks, and Foreign Banks) is detailed in paragraph 9 of the "Master Circular – Basel III Capital Regulations" dated April 1, 2024 (as amended from time to time), which would be replaced by the "Master Direction on Minimum Capital Requirements for Operational Risk" dated June 26, 2023, once the same comes into effect.
Operational Risk - Detail loss event type classification	It provides a detailed operational risk loss event type classification.	As the detailed operational risk loss event type classification has been specified in the "Master Direction on Minimum Capital Requirements for Operational Risk" dated June 26, 2023, (which REs may make use of) the same is not included in the Guidance Note.