The Digital Fifth

Decoding RBI's Guidance Note on Operational Risk Management and Operational Resilience

This document is neither a legal interpretation nor a statement of the directive. All information is posted merely for educational and informational purposes. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this document, you do so at your own risk.

PURPOSE

Financial Crisis 2007 - 09

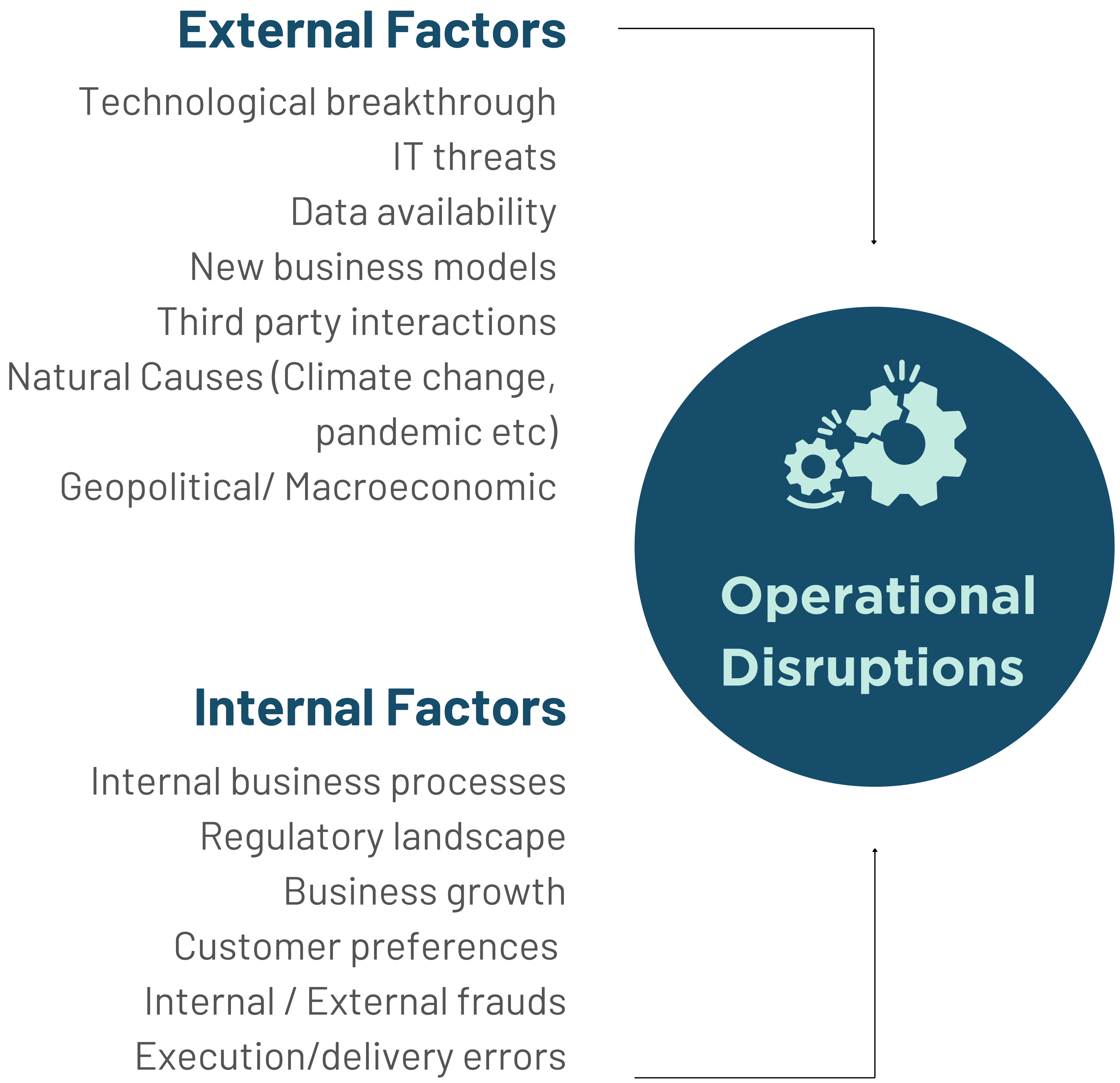
Bank's existed stress tests underestimated the impact of the crisis, prompting reforms to make them more financially resilient.

Covid'19 Pandemic

Disruption affecting information systems, personnel, facilities, relationships with third-party service providers and customers

Technological Disruption

Incidents of cyber threats, technology failures, technology adaptation challenges, High technology adoption.



External Factors

Technological breakthrough
IT threats
Data availability
New business models
Third party interactions
Natural Causes (Climate change, pandemic etc)
Geopolitical/ Macroeconomic

Internal Factors

Internal business processes
Regulatory landscape
Business growth
Customer preferences
Internal / External frauds
Execution/delivery errors

Operational Disruptions

SIGNIFICANCE OF UPDATED GUIDANCE NOTE

Particulars.	Guidance Note. 2005	Guidance Note. 2024
Focus	Operational risk management	Operational resilience as an outcome of operational risk management.
Applicability	Scheduled Commercial Banks.	All Commercial Banks, Non-Banking Financial Companies (NBFCs), Co-operative Banks, and All India Financial Institutions (AIFIs).
Organisational set up	Typical organisational setup	Regulated entities size and activity dictate their organizational setup, “typical" structure isn't applicable across.
Others	Limited /No guidance	Change management Mapping of internal & external interconnections and interdependencies Incident management Information and communication technology (ICT) Disclosures, Third-party relationships, Lessons learned and feedback

CHANGE IN THE LANDSCAPE

Technological Advancements

- Digital Transformation
- Cloud Adoption
- Fintech Integration

Regulatory Changes

- Stricter Compliance Requirements
- Open Banking

Operational Changes

- Syncronization challenges in hybrid architectures
- Unclear Product Decisions
- Processing challenges across teams

Competitive Landscape

- Rise of Neobanks
- Increased Competition from Fintech

Customer Expectations

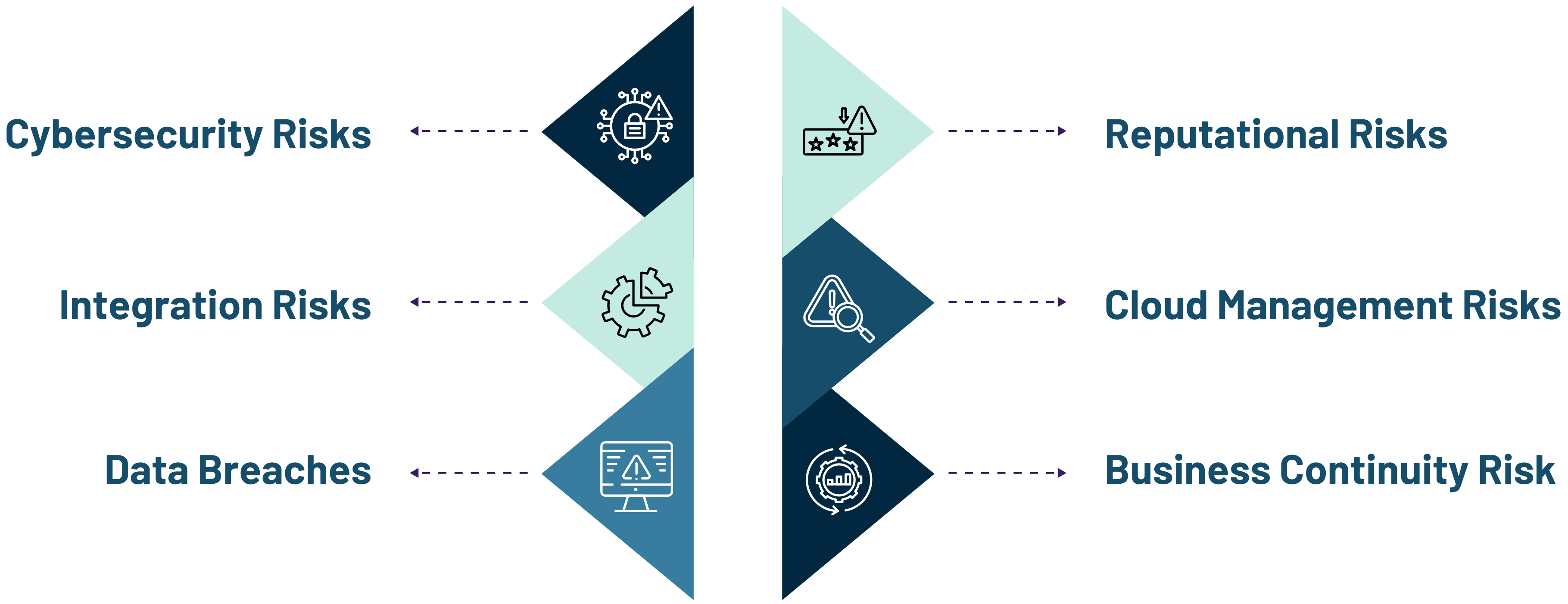
- Omnichannel Banking
- Personalization
- Real-time Services

UNDERSTANDING RISKS

Operational Risk

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.

Risk Universe



Impact if these Risks are not taken care of →

businessline.

RBI bars Kotak Mahindra Bank from onboarding new customers through online & mobile channels

businessline.

RBI action on Paytm Payments Bank has drawn fintechs' attention to compliance of laws: Minister Chandrasekhar

HDFC Bank outage: A timeline of the bank's with digital disruptions and what RBI has don

Pillar One
Prepare & Protect

- Governance & Risk Culture
- Responsibilities of Board of Directors & Senior Management
- Risk Management: Identification & Assesment
- Change Management
- Control & Mitigation
- Monitoring & Reporting

Pillar Two
Build Resilience

- BCP & Testing
- Mapping Interconnections & Interdependencies
- Third-Party Dependency Managemet
- Incident Management
- ICT including cybersecurity

Pillar Three
Learn & Adapt

- Disclosure & Reporting
- Lessons learned exercise & adapting
- Continouse improvement through feedback systems

The Digital Fifth

Pillar One:

Prepare & Protect

This document is neither a legal interpretation nor a statement of the directive. All information is posted merely for educational and informational purposes. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this document, you do so at your own risk.

THREE LINES OF DEFENCE OF OPERATIONAL RISK

The Digital Fifth

THIRD LINE OF DEFENCE: Audit Function

Independent assurance to the Board

- Identify key risk
- Review covering all activites & legal entities

SECOND LINE OF DEFENCE: Operational Risk Management Function

Smaller Regulated Entities

If functions of both first and second line of defence are combined.

Separation of duties

Independent review of processes

Larger Regulated Entities

Independent Reporting Structure

Engagement with Control groups.

FIRST LINE OF DEFENCE: Business Unit Management

Identifying inherent **products, services, activities, processes and systems risks**

Clear **roles and responsibilities** of relevant business units.

Validation

Robustness

Integrity & Credibility

Verification

Review of design, process & governance

Monitoring & Gap identification

Independent view on BUs

Risk Training and Awareness

Challenging & Measuring First line of defence

Policies, standards and guidelines.

Usage of GRC tools

Monitoring and reporting the BU's OR profiles

Establish controls

Report any residual ORs

Reporting any lack adequate resources, tools and training

GOVERNANCE & RISK CULTURE

Principle 1
Board of Directors, with help from Senior Management, should **create a strong company culture** that prioritizes risk management.

Principle 2
REs should **develop, implement and maintain an ORMF** that is fully integrated into the RE's **overall risk management processes.**

Risk Culture

Determines how individuals and groups identify, understand, discuss, and act on risks within an organization.

Accountability
at all management levels

Integration with Operational Resilience

Committees establishment

Regulatory Expectations

GOVERNANCE & RISK CULTURE

The Digital Fifth

Principle 3

Board approves and monitors operational resilience plan, ensuring senior management implements it effectively throughout the organization.

Principle 4

Board **sets risk tolerance for operational issues** and defines critical operations to improve resilience.

Roles and Responsibilities

Board of Directors

- Oversees operational risk and resilience
- Approval of the ORMF
- Construct risk appetite
- Alignment with strategic objectives.

Senior Management

- Implement approved ORMF
- Develops policies, processes, and controls
- Ensures adherence across the organization.

IMPLICATIONS

Strengthening of Governance Structures

Institutions should strengthen their governance frameworks to clarify roles, responsibilities, and accountability in risk management, potentially involving reorganization and new governance roles.

Cultural Shifts

Promoting a risk-aware culture through training, regular risk management communications from senior management, and incentives aligned with risk management goals is crucial.

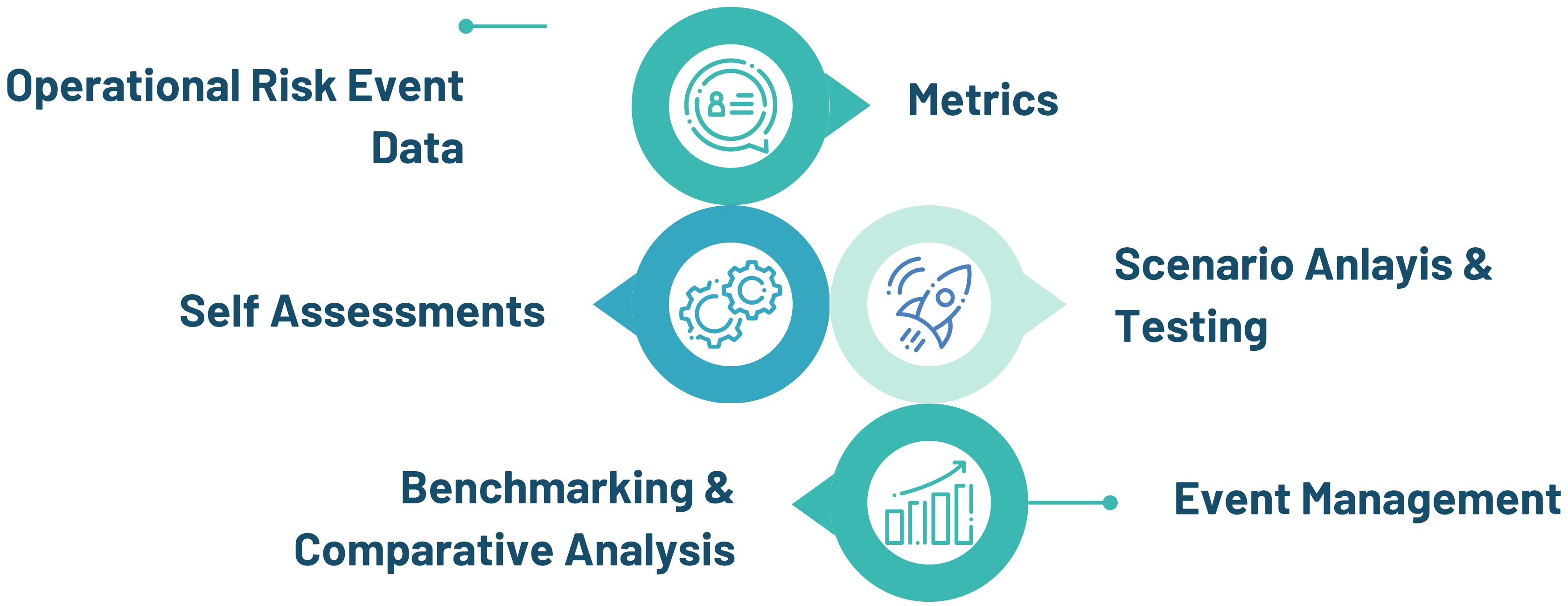
Enhanced Monitoring and Compliance

Enhanced governance will require improved internal controls and monitoring systems to ensure compliance with the new guidelines and to effectively manage operational risk.

RISK MANAGEMENT : IDENTIFICATION & ASSESSMENT

Principle 6
Senior management must comprehensively **identify and assess operational risks across all products, activities, processes, and systems**. This includes ongoing evaluation of internal/external threats and potential failures to proactively manage vulnerabilities in critical operations.

Tools for Identifying Operational Risk



Operational Risk Event Data

Metrics

Self Assessments

Scenario Anlayis & Testing

Benchmarking & Comparative Analysis

Event Management

IMPLICATIONS

Enhanced Preparedness and Agility: Organizations proactively identify risks through assessments and scenario analyses, enhancing their response to known and unexpected challenges

Improved Governance and Accountability: Clear governance structures and responsibilities bolster decision-making and adaptability to incidents, ensuring effective risk management

Data-Driven Decision Making: Utilization of data and advanced tools like AI and ML enhances risk assessment accuracy and predictive capabilities

Continuous Improvement: Organizations are advised to continually update their risk management practices to adapt to new threats and environmental changes

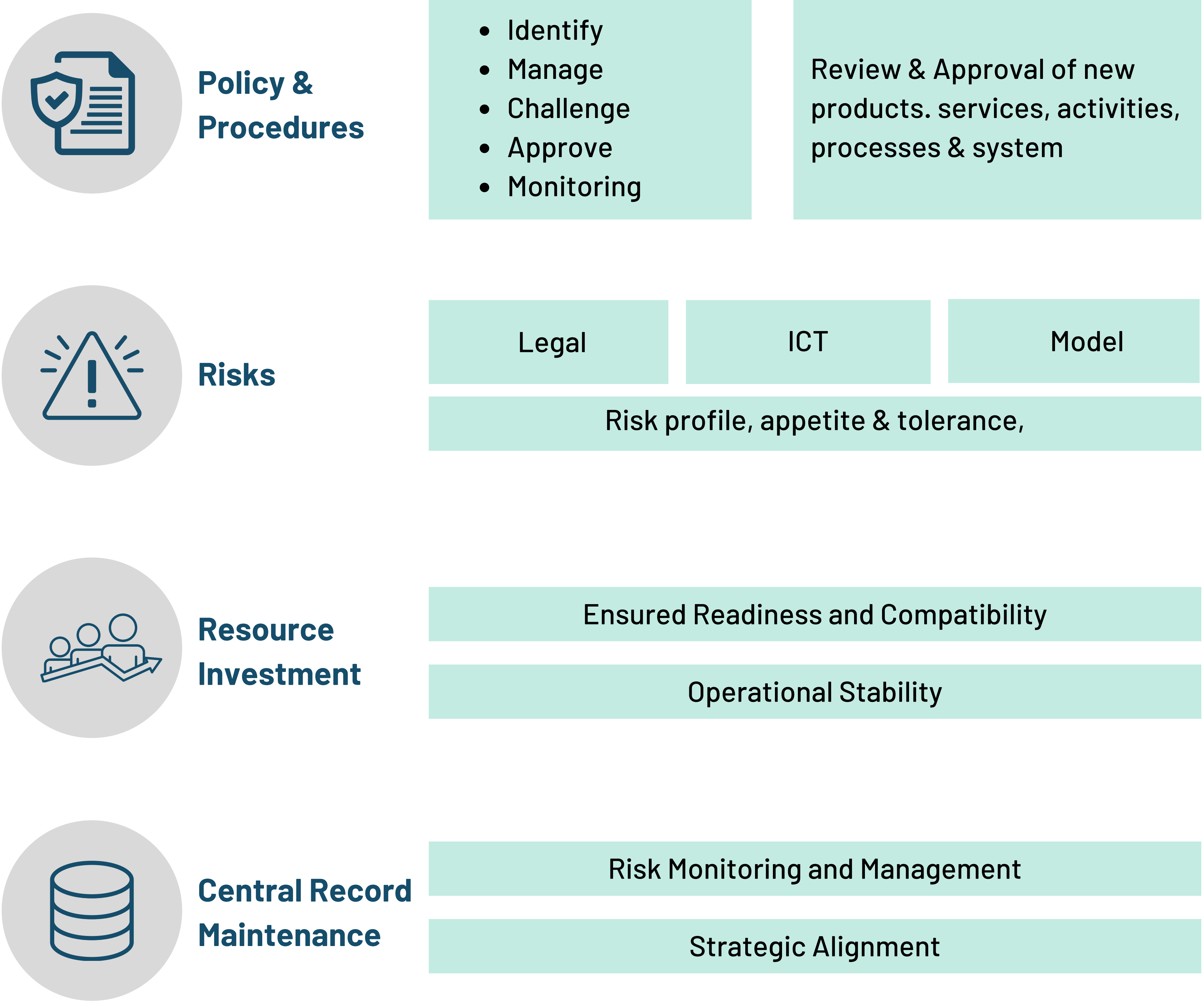
Integration with Business Continuity and IT Security: Guidelines advocate for integrating risk management with IT security and business continuity to manage interdependencies and maintain smooth operations during disruptions

CHANGE MANAGEMENT

Principle 7

Senior leadership must ensure the RE's **change management is thorough, well-resourced, and effectively communicated across** all risk control functions.

IMPLICATIONS



Policy & Procedures

- Identify
- Manage
- Challenge
- Approve
- Monitoring

Review & Approval of new products. services, activities, processes & system

Risks

Legal

ICT

Model

Risk profile, appetite & tolerance,

Resource Investment

Ensured Readiness and Compatibility

Operational Stability

Central Record Maintenance

Risk Monitoring and Management

Strategic Alignment

MONITORING & REPORTING

Principle 8

Senior management should **monitor operational risk profiles and exposures, with clear reporting to board, senior management, and business units** to proactively manage such risks.

Operational Risk Report should include:

- **Breaches** of the RE'S risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements.
- **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

IMPLICATIONS

Standardization of report
Capture key risk metrics, loss events, control effectiveness assessments, and mitigation strategies

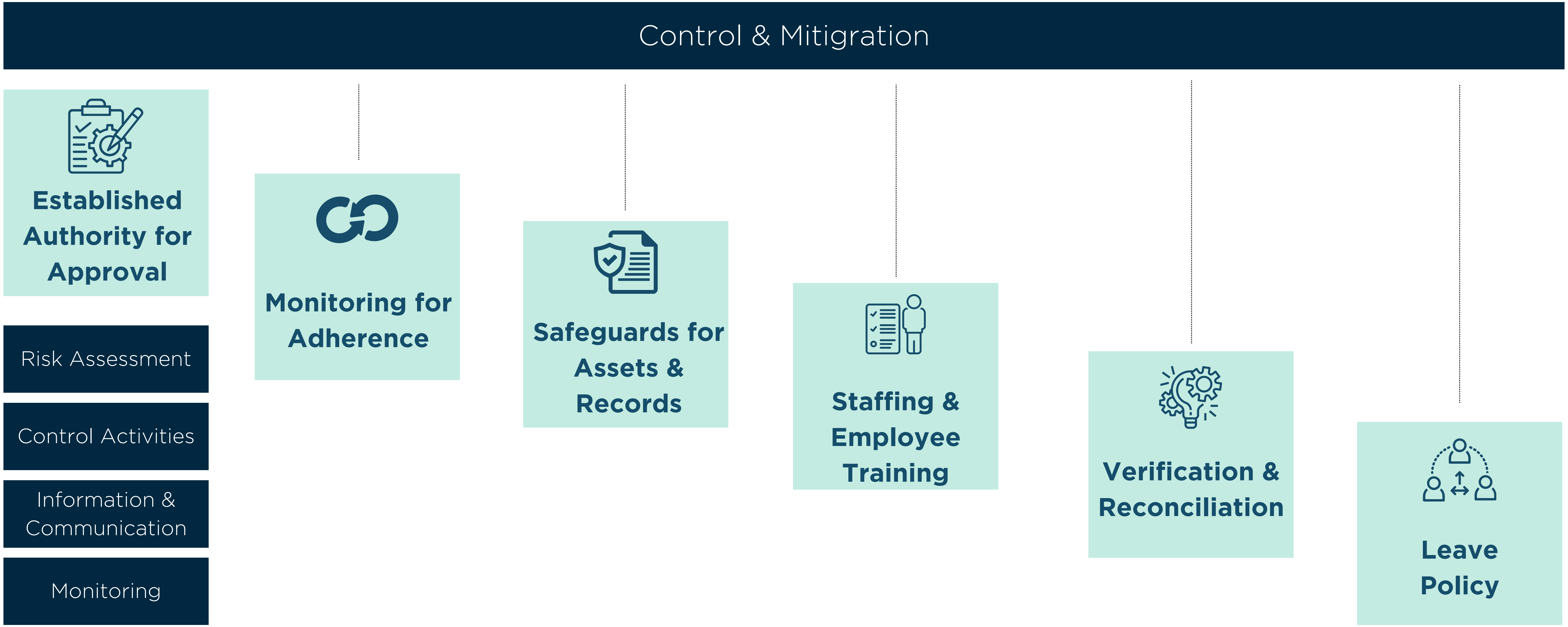
Regulatory Compliance
Adhere to relevant regulatory reporting requirements & guidelines for operational risk

Training Programs
Training on operational risk identification, assessment, and reporting procedures.

CONTROL & 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.



Control & Mitigation

Established Authority for Approval

Risk Assessment

Control Activities

Information & Communication

Monitoring

Monitoring for Adherence

Safeguards for Assets & Records

Staffing & Employee Training

Verification & Reconciliation

Leave Policy

PILLAR 1 - ACTION PLAN

STRENGTHEN INTERNAL CONTROLS

Streamlining Internal Controls

- **Policies & regulations** through reviews
- Verification
- Exception tracking.

Risk Assessment

- Continuous risk assessment
- Integration with control activities
- Information and communication systems
- Monitoring practices

ENHANCED OPERATIONAL RESILIENCE

Business Continuity Planning

Continuity of operations under both normal and disruptive conditions.

Disaster Recovery Solutions

Recovery solutions that align with the need for operational resilience and minimal disruption

COMPLIANCE AND MONITORING

Policy Compliance Assessments & Monitoring

- Evaluate compliance with management controls and the resolution of non-compliance issues.
- Monitoring systems that provide ongoing oversight of internal controls and operational risks.

SEGREGATION OF DUTIES & CONTROLS

Access Control Systems

- System for appropriate segregation of duties
- Establish dual controls to prevent losses and unauthorized actions.
- Minimize, and monitor areas of potential conflict of interest.

TECHNOLOGY & INFRASTRUCTURE RISK MANAGEMENT

Tech Governance Framework

- Identify, measure, and manage technology risks.
- Governance frameworks to address automated processes risks.
- Technology infrastructure management scrutiny.

THIRD PARTY RISK MANAGEMENT

Vendor Risk Management

- Assess risks associated with third-party service providers
- Monitor concentration of risk and managing dependencies.

Training

Comprehensive training programs for proficiency in new systems and understanding new compliance requirements.

The Digital Fifth

Pillar Two:

Build Resilience

This document is neither a legal interpretation nor a statement of the directive. All information is posted merely for educational and informational purposes. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this document, you do so at your own risk.

INTERDEPENDENCY & THIRD PARTY DEPENDENCY

Principle 10

After **identifying critical operations, an RE should map internal and external dependencies** to ensure their operational resilience approach effectively supports their delivery.

Map (identify and document)

- People
- Technology
- Process
- Information
- Infrastructure
- Interconnections & interdependencies

Principle 11

REs should **manage their dependencies on both internal & external relationships** for the delivery of critical operations

- Ownership & Confidentiality of data
- Manage & Monitor 3rd party risks.
- Contingency Plans
- Downstream service provider risks

IMPLICATIONS

Dependency Mapping
Implement sophisticated mapping of the interconnections and interdependencies for the delivery of critical operations

Identifying Vulnerabilities
Concentration risk, single points of failure, and inadequate substitutability of service providers and resources.

Risk assessment & Due diligence
To perform before entering into arrangements, whether party is consistent with its ORMF & policies

Critical Function & Downstream provider analysis
Large number of service providers are subcontracting causing supply chain vulnerabilities and lack of transparency

BUSINESS CONTINUITY PLANNING & TESTING

Principle 12

REs need **business continuity plans to be aligned with their operational resilience framework**. These plans should be tested through realistic scenarios.

Principle 13

REs to establish **response and recovery plans for critical operation disruptions**, aligning with their risk tolerance.

IMPLICATIONS

Effective governance of REs' business continuity plan requires

- Regular review and approval by the Board of Directors.
- The strong involvement of the Senior Management and business units' leaders in its implementation.
- The commitment of the first and second lines of defence to its design.
- Regular review by the third line of defence.

Inventory

Incident response and recovery

Internal and third-party resources

Classification & Prioritisation

Criteria based classification of incident's severity

Assignment of resources to respond to an incident.

Review

Periodic review of Incident response and recovery procedures

INFORMATION & COMMUNICATION TECHNOLOGY INCLUDING CYBERSECURITY

Principle 14

REs need a **robust ICT risk management program** aligned with their operational resilience framework. Ensures a secure and resilient **ICT infrastructure, including cyber security measures** with testing, situational awareness, and timely information

ICT RISK MANAGEMENT

Risk Identification and Assessment

Critical information, assets, and infrastructure.

ICT risk mitigation measures

Cybersecurity, response and recovery programmes, ICT change management processes, ICT incident management processes

Periodic monitoring of mitigation measures

ICT policy documentation

Cyber security, which stipulates governance and oversight requirements, risk ownership and accountability, ICT security measures

IMPLICATIONS

ICT Policy Framework

Comprehensive ICT policy to cover governance, oversight requirements, risk ownership, and accountability. Define ICT security measures like access controls, identity management, and protection of critical information assets.

Data Protection and Cyber Security Prioritization

Cyber security efforts based on a detailed ICT risk assessment, focusing on the protection of critical information assets.

Regulatory Compliance

ICT and cyber security implementation require legal and regulatory requirements related to data protection and confidentiality.

OPERATIONAL RESILIENCE

The capacity of financial institutions to absorb, adapt, and continue critical operations amid disruptions from operational risk events

Comprehensive Approach

Comprehensive Approach: Prepare for disruptions, respond efficiently, and recover swiftly to normalcy.

Testing and Learning

Regularly test resilience strategies and recovery plans with diverse simulations.

Governance

Emphasize the Board of Directors and Senior Management's role in fostering a strong resilience culture.

Integration with Business Continuity Plans

Integrate operational resilience into business continuity plans, covering technology, people, and processes, aligning with overall business strategies.

Regulatory Expectations

Ensure regulatory compliance for operational resilience, including reporting on resilience strategies, testing outcomes, and managing significant disruptions.

Scenario Analysis

- Identify Potential disruptions and categorise critical business operations and external dependencies.
- Impact assessments and recovery procedures

Business Continuity Procedure

- Recovery time objectives (RTO) and recovery point objectives (RPO).
- Document DR strategies and methodologies
- Communication guidelines for informing stakeholders, regulatory authorities, customers, suppliers etc.

Review & Response

- Periodic BCP effectiveness review
- Root Cause analysis
- Action Plan & Improvements

Improve

- Training and awareness programmes on Communication and crisis management to ensure continuous improvement

PILLAR 2 - ACTION PLAN

Scenario Analysis

- Identify Potential disruptions and categorise critical business operations and external dependencies.
- Impact assessments and recovery procedures

Review & Response

- Periodic BCP effectiveness review
- Root Cause analysis
- Action Plan & Improvements

Business Continuity Management

- Recovery time objectives (RTO) and recovery point objectives (RPO).
- Document DR strategies and methodologies
- Communication guidelines for informing stakeholders, regulatory authorities, customers, suppliers etc.

Improve

Training and awareness programmes on Communication and crisis management to ensure continuous improvement

The Digital Fifth

Pillar Three:

Learn & Adapt

This document is neither a legal interpretation nor a statement of the directive. All information is posted merely for educational and informational purposes. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this document, you do so at your own risk.

DISCLOSURE AND REPORTING

The Digital Fifth

Principle 15

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

Principle 16

REs should conduct lessons learned **exercises to improve their ability to adapt and respond** to future operational challenges.

Principle 17

REs should **foster a culture of learning and improvement** through effective feedback mechanisms.

IMPLICATIONS

Disclosure Policy Formulation

Develop a formal disclosure policy detailing types of Operational Risk management, tailored to the size, risk profile, and complexity

Compliance and Regulatory Alignment

Ensure all disclosure practices meet current regulatory requirements and anticipate future changes to maintain compliance and industry standards.

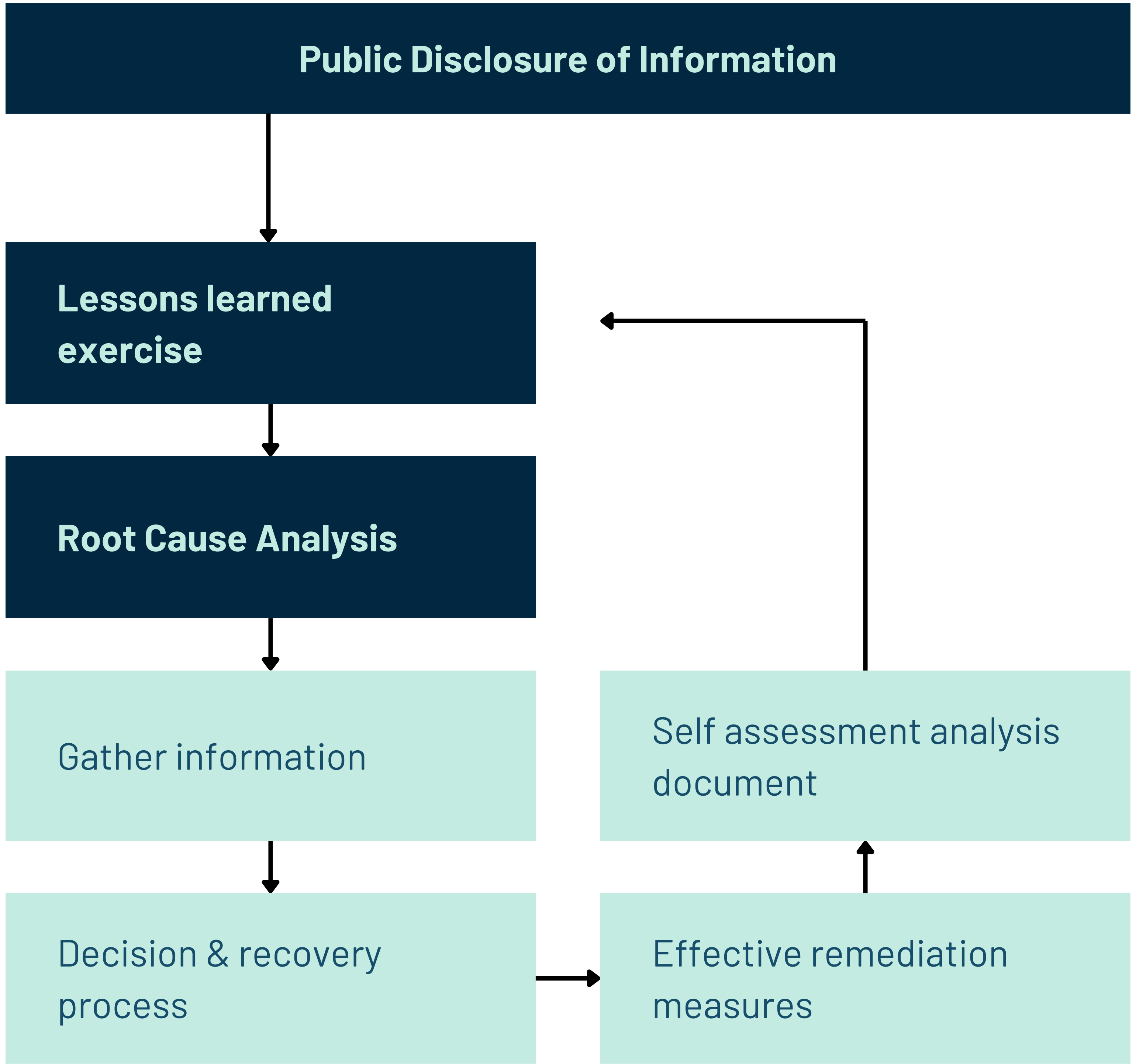
Continuous Improvement Framework

Regular reviews, performance metric tracking, and incorporating best practices learned from industry benchmarks.

Robust Feedback System

Robust feedback systems to ensure a continuous positive feedback loop fostering an effective learning environment.

PILLAR 3 - ACTION PLAN


Public Disclosure of Information
Lessons learned exercise
Root Cause Analysis
Gather information
Decision & recovery process
Effective remediation measures
Self assessment analysis document

Public Disclosure of Information - Create a policy & Communication Strategy for transparent public disclosure of risk management practices

Lessons Learned Exercise: Conduct debriefing sessions post-incident, document lessons, and update stakeholders

Gather Information: Implement a robust reporting system and feedback mechanism for employees to report and suggest improvements in risk management.

Decision & Recovery Process: Establish clear guidelines for decision-making during incidents and test through simulation & decision-making exercises

Effective Remediation Measures: Develop and prioritize action plans for remediation based on risk impact, detailing steps, resources, timelines, and responsibilities.

Self-assessment Analysis Document: Conduct regular self-assessments and update documentation to ensure compliance and reflect the latest risk management insights.

The Digital Fifth

Approach for managing Operational Risk and achieving Operational Resilience

This document is neither a legal interpretation nor a statement of the directive. All information is posted merely for educational and informational purposes. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this document, you do so at your own risk.

APPROACH TO OPERATIONAL RISK MANAGEMENT FOR ENHANCED OPERATIONAL RESILIENCE

Organizations should approach operational risk management by focusing on a holistic, integrated strategy that aligns with their overall business objectives and compliance requirements. This involves:

Integrating Risk Management with Business Processes:
Ensuring that risk management is not a siloed function but integrated with all business processes.

Utilizing Technology:
Leveraging advanced technologies for risk data collection, analysis, and real-time monitoring to enhance responsiveness.

Adopting a Proactive Stance:
Moving from reactive measures to a proactive stance in identifying and mitigating risks before they affect the organization.

Building a Culture of Risk Awareness
Cultivating a culture where all employees are aware of the potential risks and their roles in mitigating them

THE DIGITAL FIFTH APPROACH

The Digital Fifth

Identify: Initial Assessment and Risk Identification

- Evaluate existing risk management frameworks and governance structures.
- Document and assess critical business processes for inherent operational risks.
- Classify operational risks into strategic, compliance, financial, technological, and human categories.
- Perform a Business Impact Analysis (BIA) on key applications, calculating critical metrics like RTO and RPO.
- Create risk profiles based on BIA outcomes, assessing impact, likelihood, and control effectiveness.

Respond: Gap Analysis and Strategic Response Planning

- Conduct a gap analysis to assess discrepancies between current risk management practices and framework requirements.
- Formulate specific, actionable recommendations to address identified gaps and enhance controls.
- Develop a comprehensive action plan with clear timelines, responsibilities, and resource allocations.
- Ensure response strategies by integrating with BCP and aligning them with the business strategy.

Protect: Framework Development and Standardization

- Revise risk management policies to embed risk considerations in business processes per regulatory standards.
- Incorporate industry standards into the risk management framework to bolster resilience and compliance.
- Standardize the risk management framework across all units to enhance protection and streamline management and oversight.
- Leverage technology tools to automate and enforce controls, thereby reducing dependency on manual processes.

Recover: Implementation and Change Management

- Roll out new or enhanced controls and processes as per the action plan to mitigate risks.
- Set a framework for periodic reviews, audits & reporting that shall help assess the operational risk framework to the management and help take necessary adjustments.
- Help define employee roles in recovery processes to ensure swift return to normal operations after an incident.

The Digital Fifth

THANK YOU

Reach out to Us:

Deepak Sai

☎ 9704448021

✉ deepak@thedigitalfifth.com

Shashank Shekhar

☎ 9820401312

✉ shashank@thedigitalfifth.com