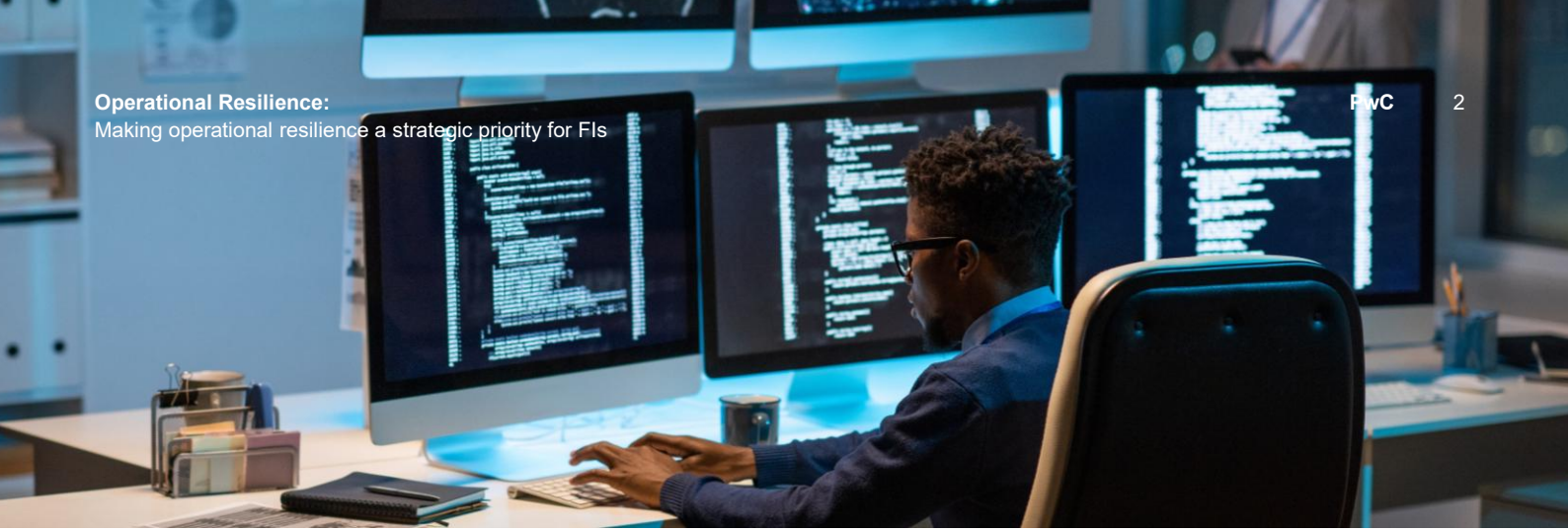
pwc

Operational Resilience:

Making operational resilience a strategic priority for financial institutions

February 2026



What is operational resilience?

Growing uncertainty, third-party reliance, and complex IT systems have heightened disruption risks and impacts, making operational resilience (OR) a business imperative for financial institutions (FIs) [1].

Traditional approaches to disruption management—such as business continuity management (BCM) and disaster recovery (DR)—have often focused on individual assets in isolation and tended to be reactive.

At its core, OR requires moving beyond a technology-centric mindset toward a business-led view—one that focuses on protecting critical services, proactively managing disruption, and ensuring continuity across the full service value chain.

This generally would require FIs to:

1	2	3	4
Prevent disruption wherever practicable	Adapt systems and processes to maintain operations in the event of incidents	Restore normal functioning promptly once disruptions end	Learn from incidents and near misses

In 2021, the Basel Committee set global standards with its Principles on Operational Resilience[1], which accept disruptions as inevitable and focus on strengthening FIs' capacity to identify, adapt, recover, and learn—thus preventing customer harm and preserving trust. As a result, OR gained momentum, with major regulatory frameworks such as the EU's Digital Operational Resilience Act (DORA) and Australian Prudential Regulation Authority (APRA) Operational Risk Management Prudential Standard reshaping approaches to resilience.

Locally, Bank Negara Malaysia (BNM) has included operational disruption measures into its BCM policy document[2] and recently issued a discussion paper outlining its emerging regulatory direction and key considerations to further strengthen the OR of FIs[3]. Although Malaysia has yet to adopt a standalone OR framework, FIs should take a proactive and holistic approach to anticipate and mitigate risks in today's increasingly complex financial landscape.

BNM's paper also emphasises that resilience is not just a FIs-level issue but an industry-wide imperative requiring collaboration. While this publication focuses on OR for FIs, it is increasingly important for other organisations to embed operational resilience within their risk management strategies.

[1] Basel Committee on Banking Supervision, "Principles for Operational Resilience", 2021
[2] Bank Negara Malaysia, "Business Continuity Management", 2022
[3] Bank Negara Malaysia, "Operational Resilience: Discussion Paper", 2025

Why is OR important?

PwC's Global Crisis and Resilience Survey 2023 reveals a stark gap: 93% of Malaysian organisations experienced disruptions in the past two years, but only 26% has an integrated resilience programme. FIs today face mounting disruption risks driven by factors such as:

A surge on ransomware attacks on government and financial institutions in Malaysia, threatening public trust, disrupting essential services, and exposing sensitive data.

Digital adoption and growing reliance on outsourced service providers creates new third-party points of failure

Resilience efforts are often managed in a fragmented way, with cyber risk, technology risk, BCM and supply chain risk addressed in silos.

OR can help FIs prevent disruptions and adapt the organisation in the face of sudden change. FIs that effectively address OR can unlock significant benefits, including lower operational costs, reduced complexity in service delivery, more efficient innovation programmes, and a better customer experience.

An enterprise-wide responsibility

OR is a critical commercial imperative requiring attention from every part of an organisation. FIs must strengthen their ability to withstand disruptions, incidents and attacks across technology, data, third parties, facilities, operations and personnel.

Since these risks affect nearly every facet of the business, operational resilience should be treated as an enterprise-wide responsibility—not confined to a single function. Ultimately, accountability rests with boards and senior management to rigorously evaluate the organisation's resilience.

Questions for board members to consider

Below are key questions boards can ask to challenge and guide management in strengthening resilience.

Strategic decision	Board-level challenge question
Cloud-first strategy	Can our critical services continue to operate if an entire cloud region fails?
Fintech / API ecosystem expansion	If a key partner or API fails, can customers still transact—and how quickly can we isolate or bypass the issue?
New digital products	Do these products introduce new dependencies or single points of failure that could widen the impact of a disruption?
Multi-country expansion	If operations in one region are disrupted, can the rest of the business continue without material impact?
Outsourcing critical processes	How resilient is our reliance on third parties, and can we switch to an alternative provider without interrupting critical services?
Cyber security enhancements	If all prevention controls fail, how quickly can we recover critical systems and data to avoid customer harm?
Data centralisation	Does concentrating data in a single hub create recovery bottlenecks or amplify the impact of a disruption?

From BCM to OR: A natural evolution

OR builds on BCM and DR to increase the focus on anticipation, prevention and adaptation to disruption.

As FIs continue to expand their service offerings, depend on complex technological systems, and increase their reliance on third-party providers for critical business functions, OR represents a natural evolution beyond traditional BCM and DR frameworks.

The table below highlights the progression from traditional approaches to BCM and DR (the 'old' way) and operational resilience (the new way).

The 'old' way	The new way
Narrowly focused on recovery of individual process(es), systems and applications	• Takes a more holistic, business services view • Prioritises customer-centric investments based on customer and market impacts • Emphasises end-to-end recovery and resumption of a business service—this includes people, process, technology, data and third-party interdependencies
Emphasis is on avoiding or preventing disruptions	• Assumes disruptions are a norm—not a question of 'if' but 'when' • Invests in reactive capabilities to recover and respond to disruptions (not just to prevent disruptions)
Ignores the role of market participants in delivering business-services	• Requires a strong understanding of third-party and related concentrations (data processors, cloud service providers, outsourcers, market data providers) that underpin a business service • Aligns third-party resilience plans and capabilities with the firm's own resilience objectives
Siloed approach between BCM/DR and related risk disciplines	• Identifies disruption scenarios for each important business service • Sets quantitative impact tolerances for disruption to important business services based on tailored scenarios

While the shift to the 'new way' of OR is the way forward for organisations, many face significant hurdles in translating these principles into practice. These challenges can be grouped into five key themes:

1. Strategic alignment

- **Embedding resilience into strategy**: Organisations often struggle to integrate resilience into core business objectives, governance, and risk frameworks
- **Resilience-by-design**: Moving beyond reactive measures to proactively designed systems and processes requires long-term investment and leadership commitment

2. Operational complexity

- **Identifying dependency:** Gaining a real-time view of critical internal and external dependencies (people, technology, facilities, third parties) is difficult in complex ecosystems
- **Data and asset management**: Rapid technology evolution and hybrid environment make it challenging to maintain accurate inventories and accountability for risks

3. Regulatory compliance

- **Keeping pace with evolving regulations**: FIs face constant changes in privacy, resilience, and third-party risk requirements, creating significant compliance pressures
- **Global standards alignment**: Harmonising local practices with international frameworks (e.g., Basel, DORA) adds another layer of complexity

4. Cultural readiness

- **Resilience-first mindset**: Staff often lack awareness of recovery processes and tools, and siloed risk management practices hinder collaboration
- **Training and awareness**: Building familiarity with resilience concepts across all levels of the organisation remains a major gap

5. Testing and assurance

- **Stress testing critical business services**: Organisations find it challenging to design and execute reliable tests for severe but plausible scenarios
- **Achieving recovery speed**: Meeting impact tolerances and recovery objectives under pressure requires robust planning and coordination

Overcoming these challenges requires a structured and practical approach. Rather than tackling resilience in silos, organisations should adopt a roadmap that translates ambition into action.

Operational Resilience Lifecycle provides this foundation, allowing organisations to embed resilience into day-to-day operations, build confidence to withstand disruption, and adapt to change.

Operational Resilience Lifecycle

01

***Important Business Services* (IBS)* identification**

Identify important business service(s)* delivered externally to the marketplace

02

Value chain process mapping

Document key processes and sequencing for the IBS, including 'critical path' processes

03

Interdependency mapping

Map underlying resources (e.g. people, technology, facilities, third-parties, upstream processes) to deliver the service

04

Impact tolerance

Set the maximum level of disruption (time based) the IBS can sustain without crossing intolerance harm to customers or triggering systemic impact.

05

Vulnerability management

Identify critical failure points that could prevent the IBS from meeting its impact tolerance

06

Resilience testing

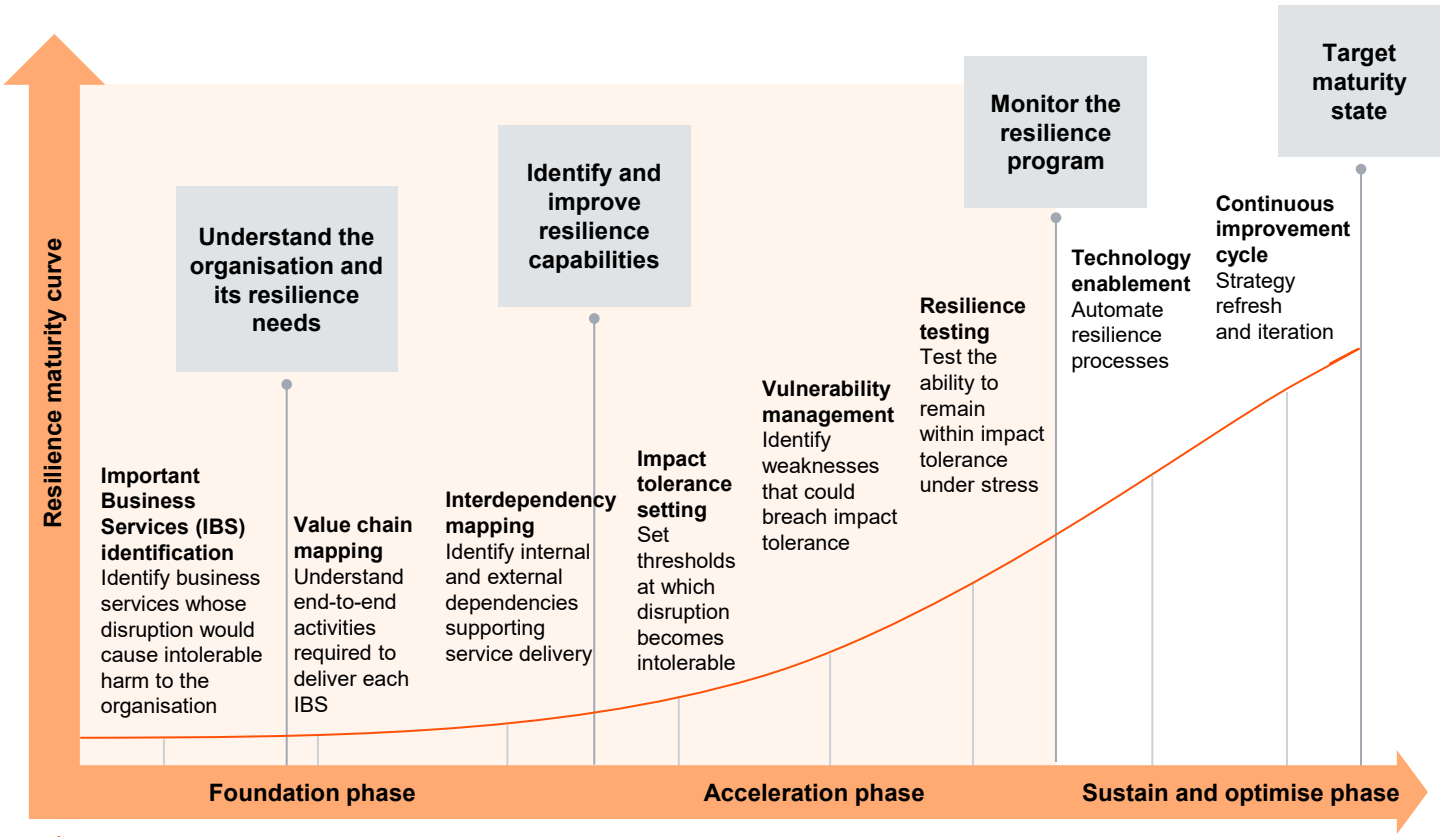
Test IBS' ability to remain within impact tolerance in severe but plausible scenarios

* *Important Business Services* (IBS)—referred to in Bank Negara Malaysia's existing policies as essential services (RMiT/BCM) and critical financial services (Operational Resilience Discussion Paper)—are the external-facing services for which disruption would result in intolerable harm to the financial institution.

OR Lifecycle: From concept to practice

OR is not a one-off compliance exercise but a progressive capability that underpins enterprise resilience. As BNM considers a standalone OR framework, FIs should start to embed OR initiatives—moving from foundational understanding to sustained optimisation—to strengthen their ability to anticipate disruption and adapt as risks evolve.

The graphic below illustrates this maturity journey, highlighting the key actions at each stage and their alignment with the themes listed in BNM's discussion paper.



Key actions

Foundation phase

- Define the universe of business services and align taxonomy
- Apply prioritisation criteria based on customer, organisational, and market harm
- Validate priorities with service owners and document exceptions

- Document key processes, sequencing, and critical path activities
- Break down activities into underlying manual and automated processes
- Identify recovery-critical steps for prioritisation during disruptions

- Map people, technology, facilities, data, and third-party dependencies
- Identify single points of failure and concentration risks
- Assess fitness-for-purpose of dependencies for resilient operations

Acceleration phase

- Define potential harms to customers, organisation, and market
- Set maximum tolerable downtime supported by volume, value, or customer metrics
- Validate thresholds with leadership and align to risk appetite

- Identify material vulnerabilities across processes and dependencies
- Differentiate resilience shortcomings from BAU operational risk issues
- Establish and track corrective action plans for material vulnerabilities

- Design severe-but-plausible, multi-day disruption scenarios
- Test multiple IBS concurrently
- Use tabletop exercises, simulations, and live recovery testing

Sustain and optimise phase

- Implement technology solutions to streamline resilience processes and introduce efficiencies

- Define priorities and implement recommendations to enhance resilience
- Refresh risk-based strategy, and implement a repeatable process to iteratively improve resilience

Alignment with themes listed in BNM's discussion paper

Preserve continuity of critical operations and/or services	Preserve continuity of critical operations and/or services	Map internal and external interdependencies	Set tolerance for disruption	Map internal and external interdependencies	Assess capabilities under severe but plausible scenarios
		Manage third-party dependencies		Manage third-party dependencies	

The bigger picture: Enterprise resilience

Enterprise resilience—the ability to anticipate, respond to and evolve through change—is essential for FIs to not only survive but thrive in today's business environment. As shown in the PwC Enterprise Resilience Framework below, it hinges on three key components:

01

Strategic resilience

The ability to evolve and adapt to emerging challenges

02

Operational resilience

The ability to maintain critical operations during disruption

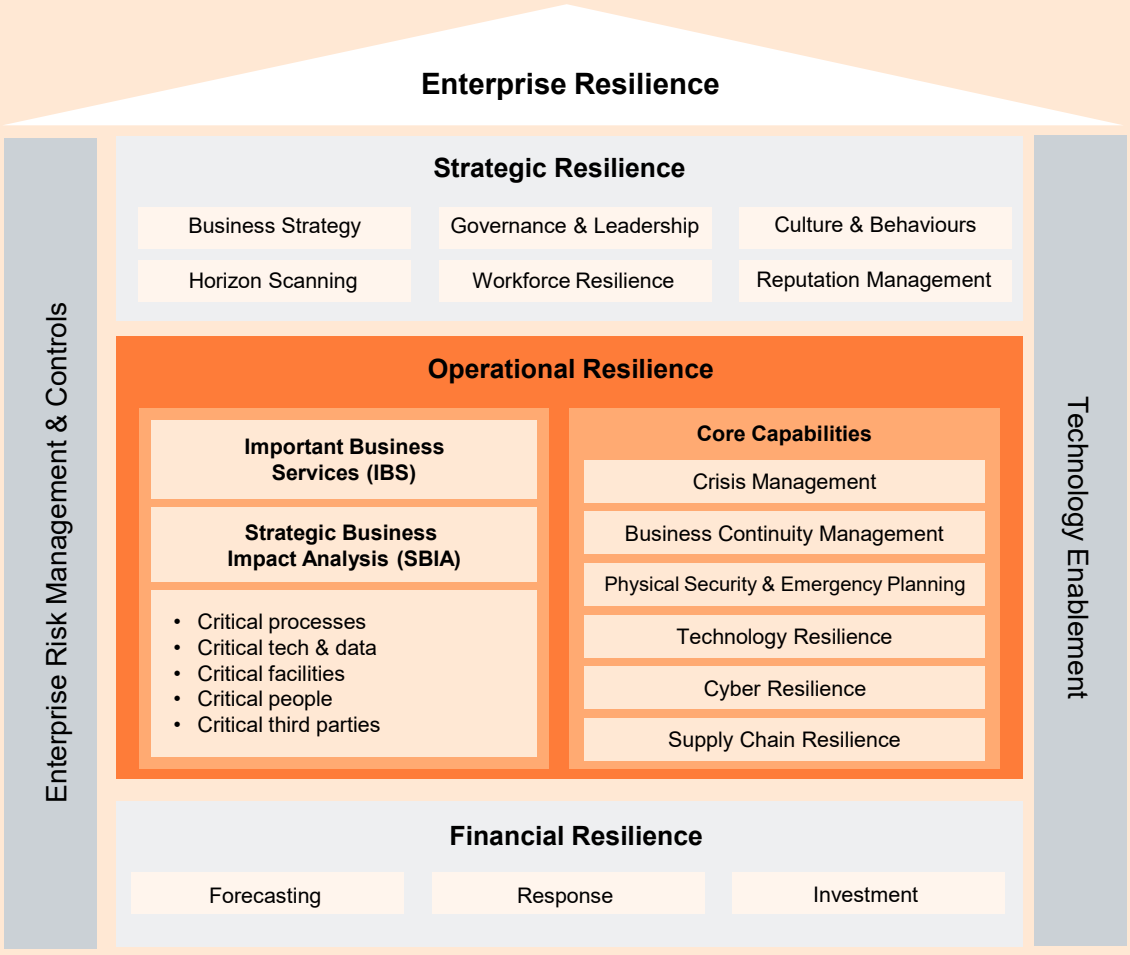
03

Financial resilience

The ability to maintain capital and cash flow during disruption

By strengthening OR, FIs reduce vulnerability while enabling quick recovery and continuous adaptability. This OR a cornerstone of enterprise resilience—empowering organisations to serve customers, support stakeholders and drive growth regardless of challenges they face.

PwC Enterprise Resilience Framework



How we can help

We bring expertise that helps you respond to disruptive scenarios to ensure the continuity of your critical business services in the following stages*:

- **Assess** the current state of your core OR capabilities and bring enhancements
- **Develop** operational resilience framework—tailored to your needs
- **Implement** the framework based on OR Lifecycle
- **Deploy** a tool with end-to-end comprehensive workflow that enables identification and mapping of dependencies, impact tolerance setting and vulnerability management

Across these stages, PwC's suite of Accelerators provides ready-made tools, templates and methodologies that help shorten delivery time while ensuring consistency and quality.

Drawing from real-world experience, our assessments will take into consideration integration and alignment of your capabilities with the overall programme strategy so that OR becomes a source of strategic confidence and competitive advantage.

**These services are non-exhaustive and can be tailored to meet specific organisational needs.*

Crisis management coordinates organisation-wide efforts to handle major events requiring executive oversight. Our services include:

- Assessing and testing your organisation's readiness to respond to crises
- Assisting in incident management from identification through recovery
- Conducting after-action reviews to improve future resilience

Business continuity ensures critical business services continue to operate during and after a disruption. Our services include:

- Identifying and reviewing your important business services and supporting resources (people, process, technology, facilities and third parties)
- Developing business continuity plans
- Conducting assessment of business continuity programme to evaluate its design and implementation

Physical security and emergency planning involves safety procedures to protect people and assets during emergencies. Our services include:

- Assessing your physical security risks with a thorough evaluation of infrastructure, personnel, travel and digital controls to identify gaps
- Developing and implementing tailored security strategies that optimise operations and prioritise investment to protect people and assets

Technology and cyber resilience focuses on safeguarding and swift recovery of IT systems during and after a disruption. Our services include:

- Evaluating infrastructure and processes through testing and validation activities
- Developing a cyber recovery plan to help facilitate a faster recovery following a cyber incident
- Monitoring dark web forums for malicious activities to identify vulnerabilities

Supply chain resilience mitigates financial, business continuity, information security and operational risk presented by third parties. Our services include:

- Independently review critical third-party arrangements for operational resilience requirements
- Assess concentration risk across supply chain, including potential offshore impacts

Financial resilience helps organisations assess and strengthen their financial capacity to withstand disruptions. Our services include:

- Financial resilience maturity assessment, governance and financial resilience framework development
- Conduct stress testing and scenario modelling simulations
- Develop and test contingency funding plan
- Review liquidity and funding gap and review capital adequacy assessment for financial institutions

At PwC, we draw on the collective skills and experience of more than 370,000 people across our network of firms in 149 countries to help build trust in society and solve important problems. We believe the opportunities of tomorrow require action today. Speak to us and explore how your business can strategically position itself to drive value and growth.

Contact us

Dominic Chegne
Partner, Risk Services Leader, PwC Malaysia
dominic.hk.chegne@pwc.com

Kelvin Lee
Partner, Financial Services Leader, PwC Malaysia
kelvin.t.lee@pwc.com

Clarence Chan
Partner, Digital Trust and Cybersecurity Leader
PwC Malaysia
clarence.ck.chan@pwc.com

Ting Choo Wai
Partner, Recovery and Response Planning, PwC Malaysia
choo.wai.ting@pwc.com

Domain specialists

Crisis, Business Continuity Management, and Supply Chain Resilience

Gayathri Jaganathan
Director, Risk Services, PwC Malaysia
gayathri.jaganathan@pwc.com

Financial Resilience

Chee Kong Chong
Director, Risk Services, PwC Malaysia
chee.kong.x.chong@pwc.com

Technology and Cyber Resilience

Alex Cheng
Director, Risk Services, PwC Malaysia
alex.ct.cheng@pwc.com