BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Operational Resilience

Discussion Paper

Issued on: 19 December 2025

BNM/RH/DP 028-25

This Discussion Paper sets out Bank Negara Malaysia's (the Bank) emerging direction and the key considerations to strengthen the operational resilience of financial institutions in a landscape marked by greater digitalisation, complex interdependencies, and more frequent and severe occurrences of operational disruptions.

The Discussion Paper seeks to–

(a) distil lessons from global and domestic operational disruptions that left widespread impact across the value chain of financial institutions;
(b) synthesise the growing convergence in thinking and the key themes/concepts around operational resilience;
(c) contextualise the key themes/concepts in Malaysia's perspective, drawing on the interlinkages with existing requirements issued by the Bank;
(d) explore and discuss the challenges and trade-offs faced by financial institutions in applying these key themes/concepts within their respective circumstances; and
(e) articulate the appropriate governance and accountability mechanisms to prompt and support more meaningful progress in elevating the operational resilience practices of financial institutions.

The Bank would like to invite written comments on the discussion areas, including suggestions and alternative approaches that should be considered. Respondents should support their feedback with clear rationale and relevant evidence or examples. In developing the written comments, respondents from financial institutions should ensure that the perspectives of their board of directors are incorporated accordingly, including in the responses to the specific questions set out in this Discussion Paper.

All written comments must be provided in the template attached and submitted via email to pfpconsult@bnm.gov.my by **30 April 2026**.

TABLE OF CONTENTS

PART A INTRODUCTION

1 Overview

1.1 This Discussion Paper sets out the emerging direction for strengthening the continuity of critical financial services in an environment shaped by rapid digitalisation, rising cyber threats, deeper third-party dependencies, and increasing severity and frequency of disruptions.

1.2 The objective of this Discussion Paper is to contextualise the changes in the landscape through discussions on:

(a) Global developments and lessons from recent international and domestic operational disruptions;
(b) Growing convergence of regulatory expectations by international standard-setters and the key themes/concepts relating to operational resilience;
(c) Operational resilience in the Malaysian context, including interlinkages with existing requirements;
(d) Challenges and trade-offs faced by the financial institutions[1] in embedding the key themes/concepts of operational resilience; and
(e) Appropriate governance and accountability structures to strengthen operational resilience.

2 Global megatrends and disruptions

2.1 A wave of technological innovation, behavioural shifts, and environmental pressures is redefining the global financial ecosystem. These megatrends have introduced new forms of operational vulnerabilities and amplified existing ones. While considerable efforts have been placed on strengthening financial resilience through strong capital and liquidity buffers in the past, recent large-scale global disruptions have made it clear that this alone is no longer sufficient to shield financial institutions from the effects of major operational disruptions. The capacity to sustain continuity of essential services under stress is now just as important as maintaining adequate financial buffers, especially as digital interdependencies continue to deepen worldwide.

[1] For the purpose of this Discussion Paper, financial institutions refer to banking institutions, Islamic banking institutions, insurers, takaful operators, prescribed development financial institutions, operators of designated payment systems, and eligible issuers of electronic money (i.e., issuers that meet the criteria outlined in the policy document on Electronic Money issued on 31 January 2025).

2.2 Operational disruptions[2] – whether arising from cyber incidents, technology failures, third-party outages, compromise of data and information assets, or power outages – can quickly lead to widespread loss of access to essential banking, insurance, takaful, and payment services. As financial services increasingly rely on real-time digital channels, cloud-based platforms, and shared external infrastructures such as telecommunication networks, the impact of outages on financial institutions, their stakeholders, and the economy has become more immediate and far-reaching.

2.3 In the current landscape, operational resilience must be viewed against the backdrop of these megatrends that are transforming the way financial services are delivered and consumed. Digital adoption in financial services continues to accelerate across retail and wholesale markets. Mobile banking, online insurance and takaful services, electronic Know-Your-Customer (e-KYC), digital onboarding, Quick Response (QR) payments, and cloud-hosted financial applications are now integral to how individuals and businesses access financial services. While cloud computing, application programming interface (API)-based integration, and open financial architectures enhance efficiency and innovation, these advancements also create complex dependency chains. This shift heightens reliance on real-time digital channels, increases sensitivity to service outages, amplifies reputational consequences of disruptions, and elevates exposure to vulnerabilities in software supply chains and interfaces.

2.4 Cyber threats remain among the most significant risks globally. The growing sophistication of attacks – including artificial intelligence (AI)-enabled exploits, ransomware, and cyberattacks targeting critical infrastructure – poses material risks to the continuity of financial services. This is evident in the shift from data thefts to cyberattacks that aim to disrupt, destruct, and destabilise systems. Global incidents highlight the growing prevalence of ransomware targeting core systems, destructive malware designed to corrupt data, attacks via third-party providers, exploitation of supply chains, and coordinated multi-entity attacks. These incidents can impair systems for extended periods of time and necessitate dynamic capabilities beyond traditional recovery measures as cyber threats continue to evolve to create disruptions that are new and unprecedented.

[2] Examples of notable disruptions globally include the IT migration failure that caused prolonged service disruptions (TSB Bank in the UK); outage of the Eurozone's core payment system and securities settlement system that halted industry-wide payment settlement, intraday liquidity transfers, and securities settlement; and the major blackout in Spain and Portugal that caused service unavailability at bank branches and self-service/point-of-sale terminals.

2.5 Digitalisation has also raised consumer expectations for uninterrupted access to financial services, where there is often little to no tolerance for downtime. This is particularly the case for access to financial services that affect consumer's ability to access their funds (such as mobile/online banking, e-wallets, or real-time payments) and, by extension, the livelihoods of the public at large. Any interrupted access to these financial services will typically trigger immediate consumer dissatisfaction, which is often amplified through social media. This in turn may threaten the reputation of the financial institution and diminish the trust and confidence of consumers, especially if the privacy of their personal information is perceived or known to be compromised (including due to fraudulent activities).

2.6 The financial system is tightly interconnected through payment networks, clearing and settlement infrastructures, shared telecommunication services, cloud ecosystems, and financial technology (fintech) and API-driven platforms. The growing dependence of financial institutions on cloud service providers, outsourced operational and IT functions, fintech partners, data centres, and telecommunication networks heightens concentration and systemic risks, where–

(a) Failures in these shared infrastructures can concurrently impact multiple financial institutions, large consumer groups, and market functions;

(b) Substitutability during outages becomes challenging when interdependencies are either opaque (where financial institutions have limited visibility into the external providers' supply chains), or when financial institutions are critically dependent on a concentrated number of service providers due to their niche/specialised services that are not easily replaceable; and

(c) Geopolitical developments and evolving legal frameworks increasingly impact technology supply chains, cloud hosting arrangements, and cross-border service dependencies, which in turn introduce operational uncertainties, complicate procurement processes, and limit diversification options.

2.7 Physical risks from climate change (including those arising from floods, heatwaves, wildfires, and storms) are affecting physical infrastructures, data centre operations, branch accessibility, and logistics networks. The increasing frequency and severity of climate events alongside other high-impact and multi-layered outages may prolong disruptions to multiple days, leading to systemic impacts across regions.

2.8 Malaysia has also experienced notable operational disruptions[3] affecting mobile/online banking channels, payment systems and switching networks, and access to automated teller machines (ATM). These incidents highlight discernible dependencies across internal systems, common industry infrastructures, and third-party providers. They also highlight challenges in managing peak loads, vulnerabilities to cyber threats, rising consumer expectations for seamless services, and the need for end-to-end operational visibility.

2.9 Across these global megatrends, instances of high-impact operational disruptions, and Malaysia's own experience, several consistent lessons emerge:

(a) Disruptions are increasingly complex and inevitable. While prevention remains key to risk management, this must be complemented with strong preparedness, adaptability, and robust recovery capabilities to enable more active and dynamic management of disruptions when they do occur.

(b) Financial institutions must identify which operations and/or services are critical to consumers and the market, and preserve the continuity of these operations and/or services.

(c) Deep visibility over both internal and external dependencies of the financial institution is essential.

(d) Impact tolerances must consider internal and external outcomes, in particular the impact to customers and stakeholders of the financial institutions, taking into account their new or heightened expectations. Internal recovery metrics of business functions and systems such as maximum tolerable downtime (MTD) and recovery time objective (RTO) remain necessary but may not be adequate.

(e) Testing for isolated failures is no longer sufficient. Scenario testing must be severe enough yet still reasonably plausible, incorporating concurrent scenarios to form a realistic view of vulnerabilities and failure events.

(f) Strong board oversight, alongside timely decision-making within a cross-functional and integrated set-up, is a critical differentiator between financial institutions that can withstand disruptions and those that struggle to do so.

(g) Continuous improvement and learning are essential, whereby financial institutions must establish a structured process to integrate lessons and insights from every disruption into future planning. Financial institutions that consistently learn from incidents are likely to improve at a faster pace.

[3] Some recent examples include mobile application outages due to inadequate mainframe storage in core banking systems that prevented QR payments and fund transfers, outage of core banking services that left most banking services disrupted (branches, ATMs, and internet banking) following a failed disaster recovery test, and a ransomware attack due to weak cybersecurity controls, i.e., obsolete servers and the absence of multi-factor authentication.

3 Convergence of understanding on operational resilience

3.1 Taken together, the megatrends and disruptions demonstrate a clear shift in how operational resilience must be approached. The lessons are reflected in the direction that international standard-setters have taken in recent years, most notably in the publications on operational resilience by the Basel Committee on Banking Supervision (BCBS)[4] and the International Association of Insurance Supervisors (IAIS)[5].

3.2 While the framing and emphasis may be different due to the sectoral focus in the respective publications by BCBS and IAIS, operational resilience is commonly understood and grounded on the shared recognition that disruptions are inevitable. This is a key assumption that is put forth to shape the operational resilience of a financial institution, defined by the ability of their critical operations and/or services to withstand disruptions within acceptable and tolerable levels under severe but plausible scenarios. Of importance, being operationally resilient is seen as the outcome of strong governance, effective operational risk management, robust business continuity arrangements, and active management of internal and external dependencies.

3.3 This reflects a convergence in thinking and a shared understanding of what financial institutions must be capable of delivering, which can be summarised into common themes and foundational elements of core capabilities of financial institutions to–

(a) **Preserve continuity of critical operations and/or services**
Not all operations and/or services carry equal significance. With the assumption that disruptions are inevitable, financial institutions must be able to prioritise the ability to continue delivering what is essential and critical to its customers and stakeholders. Failures in delivering these critical operations and/or services can adversely impact customers and other stakeholders, create contagion risks, and undermine confidence in the financial institution and the financial industry;

(b) **Map internal and external interdependencies**
Disruptions can propagate through a complex network of people, processes, data, technology, facilities, and business units. A financial institution cannot protect its critical operations and/or services without understanding what it relies on and how failures propagate. Mapping the interdependencies will facilitate identification of vulnerabilities and critical points of failure arising from any weaknesses in risk controls and the

---

4 Principles for operational resilience issued on 31 March 2021 by BCBS.
5 Draft Application Paper on Operational Resilience Objectives and Toolkit issued on 1 July 2025 as part of IAIS' consultative process.

concentration and interlinkages of systems, processes, functions, and external service providers;

(c) **Manage third-party dependencies**
As financial institutions increasingly rely on third-party service providers (including cloud and data processing providers, outsourcing arrangements, third-party administrators, and distribution partners), disruptions at these service providers will lead to delays in recovery or systemic risks. It is therefore important for financial institutions not to confine their considerations on the dependencies within their own organisation but to expand their considerations more broadly towards the wider ecosystem in which they operate in, to ensure robust contingency plans and pre-determine viable alternative arrangements for critical third-party services in the event of outages;

(d) **Set tolerance for disruption**
Financial institutions must set a clear understanding on the boundary between what is acceptable and what is not, particularly when harm is caused (e.g., towards their customers or the financial system). This includes how long critical operations and/or services can be disrupted, how much impact is allowable before customers or markets experience harm, and what level of operations and/or services must be maintained at minimum under disruptions to guide prioritisation of resources; and

(e) **Assess capabilities under severe but plausible scenarios**
While historical experiences can be used as proxies to predict future and emerging risks, it is crucial for financial institutions to understand the capabilities of their critical operations and/or services to withstand disruptions across a broad range of scenarios that are severe enough to reveal deficiencies, yet remain credible to materialise. This includes challenging their assumptions, anticipating multi-layered failures, and validating the ability of their critical operations and/or services to endure such scenarios, which can in turn be helpful for the financial institutions to calibrate their tolerance for disruptions.

3.4 Central to these key themes are the leadership and culture within financial institutions. Boards and senior management are expected to take clear ownership by ensuring that critical operations and/or services are understood, adequately resourced for, and supported by robust oversight across technology, operations, and risk functions. This includes making informed decisions about outsourcing, technology investments, and recovery capabilities, with a fuller appreciation of their implications on the financial institutions' operational resilience.

3.5 Operational resilience is not a one-off exercise – it is a continuous journey that requires financial institutions to learn from disruptions and near misses in the evolving threat landscape. Periodic reviews, updated testing, and improvements to processes, architecture, and governance structures are expected to ensure that the operational resilience of financial institutions keeps pace with the changing environment.

PART B DISCUSSION AREAS

4 Operational resilience in Malaysia's context

4.1 Around the world, several high-impact outages have demonstrated how digital financial ecosystems – no matter how advanced – remain vulnerable to sudden system failures with widespread economic consequences. The series of major operational disruptions in Malaysia[3] must be viewed in this broader global context, reinforcing the need for players in the Malaysian financial system to shift decisively from a recovery-focused approach to a resilience-first approach that is more forward-looking.

4.2 Over the years, the Bank has purposefully built a complementary set of policies[6] designed to address distinct needs, including ensuring that financial institutions maintain clear oversight structures, sound risk management practices, robust systems, and well-managed third-party arrangements. These requirements are intended to enable financial institutions to sustain critical services and restore normal operations promptly following disruptions. While these requirements already embed elements of the common themes described in paragraph 3.3, it is an opportune moment for financial institutions and the Bank to assess and review the extent of implementation of these key elements and take appropriate steps to strengthen practices of the financial institutions, where needed.

4.3 In the context of preserving continuity of critical operations and/or services, the Business Continuity Management (BCM) policy document requires financial institutions to identify critical business functions, which among others, is meant to support the continuity of their essential customer-facing services. The BCM policy document also requires the establishment of business continuity objectives, including MTD and RTO, in line with the risk appetite of financial institutions. This is complemented by more granular requirements on technology risk under the Risk Management in Technology (RMiT) policy document to ensure that the technology architecture is designed to be robust, with high availability, and is capable of withstanding disruptions.

4.4 The BCM policy document also requires financial institutions to have in place processes to identify and assess the various internal and external interdependencies (including the mapping of people, processes, and technologies). Outsourcing and third-party arrangements that support critical business functions must be captured in the business continuity planning and properly documented to ensure that financial institutions have visibility and retain

---

[6] These policy documents include Business Continuity Management issued on 19 December 2022, Risk Management in Technology issued on 28 November 2025, Outsourcing issued on 23 October 2019, Operational Risk issued on 11 May 2016, Responsibility Mapping issued on 29 December 2023, Risk Governance issued on 1 March 2013, and Corporate Governance issued on 3 August 2016.

ultimate control over dependencies, even when these are outsourced. The RMiT policy document also requires due diligence on technology dependencies, particularly on cloud services and third-party providers, to ensure these arrangements are subject to adequate risk controls.

4.5 To manage risks from external dependencies (including reliance on niche/specialised services by third-party service providers), the Outsourcing policy document currently requires financial institutions to conduct risk assessment and due diligence, execute outsourcing agreements and incorporate contractual terms, establish contingency plans to manage any failures of the service provider (e.g., engaging an alternate service provider), and maintain a register of outsourcing information. For engagements with technology-related service providers, the RMiT policy document further supplements these measures by mandating risk assessments throughout the engagement with technology-related service providers, inclusion of adequate rights of access by the financial institution and the Bank as well as business continuity capabilities within the service level agreements, and continuous monitoring of the provider's cybersecurity posture.

4.6 Within Malaysia's context, requirements are articulated with a varying degree of prescriptiveness and principle-based focus. This is intentional to reflect the risk sensitivity and operational realities of financial institutions as observed by the Bank, where certain domains require uniform minimum baselines to ensure stability across the financial sector, while other requirements are articulated with a degree of flexibility to accommodate differences in business models, operational structures, and risk appetite.

4.7 Requirements on technology and third-party risk management are relatively more prescriptive because technology failures, cyber incidents, and disruptions in critical third-party arrangements can result in high-impact consequences that propagate quickly through the financial ecosystem. These risks exhibit a very low tolerance for error, as they involve shared infrastructure and common vendors which can quickly degrade public confidence if not managed to a consistent technical baseline. In particular, the RMiT policy document sets clear requirements that are fundamental for the continuity of services, particularly in relation to system availability, security controls, recovery capability, and failover arrangements.

4.8 In contrast, requirements in the BCM, Corporate Governance, Risk Governance, and Responsibility Mapping policy documents adopt a more principle-based approach, given that these requirements emphasise judgement, behavioural expectations, oversight quality, and organisational accountability. These are areas that benefit from some degree of flexibility due to diversity across financial institutions. The BCM policy document allows financial institutions to determine

appropriate recovery strategies for critical business functions. Governance-related policy documents deliberately avoid prescribing structural configurations, and instead focus on roles, responsibilities, and decision-making effectiveness – domains where prescriptive rules are not desirable, except where warranted.

4.9 This differentiated approach ensures that standardisation is applied where uniformity is essential, while proportionality and flexibility are preserved where outcomes depend on context-specific judgement. The Bank expects that this calibration will remain appropriate in the short- to medium-term, given the systemic importance of technology and third-party risks, as well as the continued evolution of the financial sector.

4.10 However, the Bank acknowledges that the degree of prescriptiveness or principle-based focus should not be static. Over the medium- to long-term horizon, policy requirements and supervisory expectations may evolve to be in line with the developments and advancements in the industry, demonstrated through strengthened practices in identifying critical operations and/or services, managing internal and external dependencies, strengthening third-party oversight, assessing capabilities under severe but plausible scenarios, and setting clear tolerances for disruptions. Conversely, if gaps persist or new vulnerabilities emerge, the Bank will maintain or strengthen prescriptive requirements where necessary to safeguard the stability of the financial system and public confidence.

4.11 As the Bank considers the next stage of enhancements to strengthen financial institutions' ability to manage disruptions in an increasingly digital and interconnected environment, the Bank is exploring whether to incorporate a more explicit articulation of operational resilience within the existing regulatory framework, or to create a new standalone construct of operational resilience to complement the existing requirements as organising principles. This is intended to introduce and promote structured understanding of what it means for financial institutions to be operationally resilient.

4.12 This proposed articulation is not intended to displace existing requirements. Instead, it acknowledges that financial institutions have already developed approaches on:

(a) Business continuity planning, where financial institutions must identify key business functions and plan for their restoration;
(b) Technology governance, with established baseline requirements for system availability and cyber preparedness;
(c) Third-party management that are subject to adequate safeguards and continuity provisions;
(d) Operational risk management that captures and mitigates vulnerabilities across people, processes, systems, and external events; and

(e) Governance and responsibility mapping that ensure oversight and accountability for these areas at the board and senior management levels.

In the context of operational resilience, framing these elements under a clearly defined outcome therefore provides structure and coherence to practices that financial institutions can embody, while fostering greater alignment between supervisory expectations and industry implementation.

Questions for feedback

1. Please describe how your financial institution currently determines which operations and/or services are most essential to customers and the proper functioning of the market (e.g., interbank liquidity, funds and securities settlement, etc.).
2. How does your financial institution map the dependencies between business, technology, and other relevant components for an end-to-end view that facilitates the continuity of critical operations and/or services in the current environment?
3. What is the appropriate level of mapping granularity and other areas of harmonisation that would enable practical comparability, consolidation, and a streamlined view within your financial institution?
4. Please describe the challenges faced by your financial institution in ensuring continuity of critical operations and/or services that depend on third-party services, particularly in relation to substitutability and alternative arrangements in the event of disruptions.
5. Please describe the extent to which your financial institution's current practices embed the concept of severe but plausible scenario, and how previous scenario designs succeed or fail in revealing vulnerabilities across systems, people, processes, and third-party arrangements.
6. What considerations should guide your financial institution's establishment of tolerances for disruptions, and how would your financial institution ensure that these tolerance levels inform decision-making, resource allocation, and recovery priorities?
7. In embedding the definition and key themes described in paragraph 3.3 in your financial institution, please describe whether there are areas that may conflict with your existing practices or the existing requirements issued by the Bank.
8. Please discuss whether a standalone construct of operational resilience as organising principles (distinct from the existing requirements) is necessary, or whether the existing requirements sufficiently consider the key themes described in paragraph 3.3.
9. How should the application of the definition and key themes of operational resilience differ in the context of your financial institution, particularly in terms of your business model, size, complexity, and reliance on technology?

5 Trade-off in strengthening operational resilience

5.1 Strengthening operational resilience requires organisational alignment, long-term commitment, and sustained momentum to drive improvements (including investment and capital expenditure). However, financial institutions operate within governance structures, commercial incentives, and market conditions that shape how operational resilience is prioritised in practice. The Bank recognises that financial institutions often face a range of inherent trade-offs, i.e., between cost and operational resilience, innovation and safety, transparency and reputational concerns, and institutional priorities and system-wide expectations.

5.2 A central trade-off arises between the long-term investments necessary for operational resilience and the short-term pressures associated with commercial performance and operational efficiency. Enhancing system architecture, strengthening redundancy, upgrading monitoring capabilities, and improving failover arrangements require significant capital expenditure and may not yield immediate financial returns. These investments can be difficult to prioritise within budget cycles, particularly where shareholder expectations emphasise near-term profitability and where resilience spending is not directly visible to customers. As a result, financial institutions may not direct appropriate attention or investments in core capabilities needed to elevate their operational resilience unless minimum regulatory baselines (though more granular and prescriptive requirements) are established and reinforced through accountability frameworks.

5.3 The governance dimension introduces a second trade-off, where boards and senior management are expected to provide clear tone from the top, yet must also engage in increasingly complex technical discussions that underpin the resilience of technology environments. While strong governance intent is necessary, it may not be sufficient if boards are not equipped or provided with the necessary support to facilitate adequate technical understanding or knowledge to anticipate megatrends that might threaten the resilience posture, challenge architectural decisions, interpret operational resilience indicators, understand implications of third-party dependencies, evaluate robustness of scenario testing designed to validate recovery capabilities, or evaluate whether proposed solutions are comprehensive and genuinely strengthen the end-to-end delivery of critical operations and/or services. This gap can create blind spots, weaken oversight, and undermine the alignment between governance expectations and operational realities.

5.4 Within financial institutions, there may be potential misalignment of incentives and frictions between the first and second lines of defence. For example, senior officers such as Chief Operating Officer (COO), Chief Technology Officer (CTO), and Chief Information and Security Officer (CISO), depending on the specific context of the organisation and governance structure of the financial institutions, may be evaluated on metrics of cost efficiency, timely delivery of initiatives, or incident

minimisation. While important, these incentives can unintentionally discourage transparency, early escalation of weaknesses, investment in preventive controls, or trigger execution of contingency measures. At times, operational pressures or reputational concerns may also lead to downplaying near misses or delaying critical remediation actions. Conversely, the second line of defence functions may struggle to influence decision-making or insist on structural fixes when immediate business needs dominate. These dynamics can reduce the effectiveness of governance frameworks and impede a holistic approach to resilience.

5.5 From the broader industry standpoint, financial institutions face another trade-off between optimisation at the individual financial institution level and collective operational resilience at the industry level. Decisions made by a single financial institution (such as selecting low-cost vendors or designing resilience standards below the industry frontier) can create systemic vulnerabilities when financial institutions are interconnected through common payment systems, digital platforms, or cloud service providers. While financial institutions may view investments on their operational resilience as a private cost unique to their respective financial institution's circumstances, the benefits of these investments often accrue to consumers, counterparties, and the broader financial system. This disconnect can result in underinvestment at the system level if financial institutions act independently.

5.6 Furthermore, the growing reliance on common third-party and outsourced service providers heightens the importance of sector-wide collaboration. As financial institutions on their own may have limited leverage to negotiate stronger service-level commitments, enhanced recovery capabilities, and greater assurance mechanisms[7], collective engagement is increasingly necessary to establish minimum expectations for security, service availability, continuity, and incident management. Developing industry-wide technical baselines, supported by shared principles and consistent engineering or service-level expectations, would enable financial institutions to present a unified position when dealing with critical third-party service providers and ensure more predictable operational resilience outcomes across the sector.

5.7 These institutional and industry-level trade-offs must also be considered against the broader policy objectives of financial stability and consumer protection. Short service disruptions that may appear tolerable from a commercial perspective can cause outsized harm to consumers during peak period (such as salary credits or major retail events) and these can undermine trust in financial services. The highly interconnected nature of Malaysia's payment and financial market infrastructures means that disruptions at even a single financial institution can propagate quickly,

[7] For example, pooled audit, independent third-party audit, and industry certifications.

affecting businesses, merchants, and the proper functioning of the wider economy. As the operational resilience of individual financial institutions is inseparable from the resilience of the overall system, it is imperative for financial institutions not to only consider the continuity of critical operations and/or services across a range of scenarios that reflect the changing nature of operational risk, but also recognise that this can be viewed as a strategic enabler as it underpins the financial institution's ability to deliver reliable, uninterrupted services and maintain consumer trust.

5.8 Taken together, these trade-offs underscore the need for more deliberate and collaborative efforts from the financial industry. As operational resilience becomes increasingly central to public confidence in financial services, it is neither sustainable nor appropriate for financial institutions to depend primarily on regulatory intervention. Operational resilience is a shared responsibility, and the financial industry must demonstrate stronger leadership in addressing structural weaknesses, aligning incentives, and elevating resilience practices to reflect the critical role that financial services play in the economy. While the Bank continues to set supervisory expectations, issue relevant requirements, and monitor compliance, meaningful and lasting progress requires financial institutions to step up collectively and strengthen governance oversight, adopt robust risk management practices and standards, and work together to address common vulnerabilities, including through coordinated engagements with critical third-party service providers and collaboration among industry players across the different sectors[8].

[8] There are examples of coordinated efforts in the UK that seeks to promote more coordinated initiatives on operational resilience, including identification of risks to the operational resilience of the financial sector, developing solutions, and sharing knowledge across the financial industry.

Questions for feedback

10. What is the key trade-off that your financial institution finds hardest to balance, and which are the top three considerations in your financial institution?
11. What measures can financial institutions consider to better align internal incentives with desired outcomes for operational resilience?
12. Are there currently any performance metrics, key performance indicators, or internal escalation practices that may unintentionally discourage early identification or transparent reporting of vulnerabilities?
13. Are there any particular types of investments (e.g., architecture redesign, enhanced monitoring, redundancy, testing for operational resilience, etc.) where clearer regulatory expectation would support more consistent prioritisation?
14. What mechanism would support stronger collective industry engagement with critical third-party service providers? How can information sharing on operational disruptions, near misses, or emerging vulnerabilities be improved while maintaining confidentiality and trust among the industry?

6 Governance and accountability structures for operational resilience

6.1 Operational resilience must be made a board-level priority due to the growing frequency and severity of disruptions which can cause intolerable harm to customers and threaten financial stability. Boards play a crucial role in overseeing operational resilience, including approving critical operations and/or services, setting impact tolerances for disruptions, reviewing resilience testing results, and holding senior management accountable for resilience outcomes. To meet these expectations, boards need to enhance their expertise, challenge senior management effectively, integrate resilience considerations into strategy and resource allocation, and establish clear governance and accountability structures for operational resilience.

6.2 Operational resilience spans across various domains such as technology, risk management, operations, business, outsourcing, and cybersecurity. Its cross-functional nature requires a holistic approach, as working in silos can lead to organisational blind spots and may impede the board's ability to have an integrated oversight of operational resilience.

6.3 The Responsibility Mapping policy document, which will come into effect on 1 January 2026 mandates financial institutions to designate a member of senior management with a direct reporting line to the Chief Executive Officer (CEO) as responsible for implementing the operational resilience framework. While the Bank expects a single person to be ultimately accountable for operational resilience outcomes, other members of senior management share the responsibility for delivering operational resilience outcomes in their respective domains (for

example, CTO for technology resilience, CISO for cyber resilience, COO for process resilience, Chief Risk Officer (CRO) for risk appetite, and heads of business units for critical services).

6.4 Centralised accountability ensures, among others:

(a) Stronger cross-functional coordination within the financial institution during both business-as-usual and crisis conditions;
(b) Integration of resilience considerations into strategy, business, and outsourcing decisions;
(c) Robust management of trade-offs between resilience versus cost, innovation, efficiency, customer experience, business growth, and risk appetite;
(d) Timely escalation of issues and remediation of identified weaknesses;
(e) Consistent, structured, and forward-looking reporting on operational resilience risks; and
(f) More effective incident response and crisis management.

Questions for feedback

15. What are the challenges faced by the board in overseeing operational resilience (e.g., technical understanding, information quality, clarity on role and accountability, timeliness and sufficiency of incident reporting)?
16. On technical literacy, what forms of support, capacity building, and reporting structures would help boards and senior management engage more effectively on discussions related to operational resilience?
17. Please provide your financial institution's views on having a single accountable person ultimately accountable for operational resilience. In addition, please describe how this will or will not improve the board's oversight on operational resilience, including any appropriate alternative governance arrangements.
18. Which member of senior management is most suited to be made ultimately accountable for operational resilience outcomes and why?
19. Do you plan to have a dedicated Chief Operational Resilience Officer? Explain the reason for your answer.

7 Future direction and priorities

7.1 Strengthening operational resilience is now an essential priority for safeguarding consumer trust, preserving financial stability, and ensuring the continuity of critical operations and/or services in an increasingly digital and interconnected landscape. Malaysia's financial sector is well-placed to advance this, building on the foundations set out by the existing requirements and practical experience gained from past disruptions. However, global developments and domestic trends will need to continue to be considered more holistically with an outcome-focused

approach – one that is anchored on critical operations and/or services, informed by deep visibility of dependencies, supported by strong governance, reinforced through realistic scenario testing, and continuous improvements.

7.2 Looking ahead, the Bank's direction is guided by the principle of proportionality, parity, and neutrality with considerations of practical implementation for the financial industry. The Bank remains open to refining existing policy requirements including clearer articulation of critical operations and/or services, alignment of impact tolerance concepts, more guidance and standards on dependency mapping and third-party service providers, improved incident communication outcomes, or enhanced surveillance of technology and third-party risks, if necessary.

7.3 This Discussion Paper serves as the starting point for engagement between the Bank, financial institutions, and critical service providers. The Bank invites open and constructive feedback on the practical challenges, readiness considerations, and opportunities for improvements toward a more operationally resilient financial sector.