BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 1203

Series of 2024

Subject: Guidelines on Operational Resilience

The Monetary Board, in its Resolution No. 1170 dated 10 October 2024, approved the guidelines on operational resilience in line with the Bangko Sentral's thrust to foster continuous delivery of services to support inclusive and sustainable economic growth. The guidelines aim to promote and strengthen the Bangko Sentral Supervised Financial Institutions' (BSFIs) ability to manage and mitigate the impact of disruptions, particularly on their critical operations.

Section 1. Section 146/146-Q of the Manual of Regulations for Banks (MORB)/Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) on "Operational Risk Management" are hereby retitled[1] and amended to incorporate the guidelines on operational resilience, and shall now read, as follows.

146/146-Q OPERATIONAL RISK MANAGEMENT AND *OPERATIONAL RESILIENCE*

I. Operational Risk Management

xxx

Supervisory enforcement actions. xxx. Sanctions may likewise be imposed on a bank/QB and/or its directors, officers and/or employees.

II. Guidelines on Operational Resilience.

Policy Statement.

Consistent with the Bangko Sentral's mandate to promote financial stability, the Bangko Sentral aims to strengthen the operational resilience of its supervised financial institutions or their ability to manage and mitigate the impact of disruptions on their critical operations, to support the smooth functioning of the real economy.

Scope of Application

The guidelines on operational resilience shall apply to all BSFIs[2]. BSFIs shall prepare their operational resilience framework on a solo and group-wide basis, as applicable. The group-wide operational resilience framework shall encompass the parent bank/QB and all its material entities, including subsidiary banks/QBs. In the design of its operational resilience framework, the BSFI shall consider the key elements and principles embodied in this Section. Foreign bank branches may refer to the operational resilience framework of their respective Head Offices and adopt relevant policies and procedures that are consistent with the applicable

[1] All references to Section 146/146-Q where the title of the Section was mentioned should be replaced with the amended title.

[2] Including non-bank e-money issuers (EMIs) but excluding designated payment systems, financial market infrastructures that are interconnected to designated payment systems and registered operators of payments systems who serve as critical service providers unless these operators are also BSFIs.

provisions of this Section and commensurate with the scale of their operations in the Philippines.

Definition of Terms[3]

a. *Operational resilience* is the ability of a BSFI to deliver critical operations through significant operational disruption. This encompasses the BSFI's ability to identify and mitigate threats and potential failure, plan, respond, restore, and learn from disruptive events to minimize impact on delivery of critical operations through disruptions.

b. *Critical operations* include critical functions and involve activities, processes, services and their relevant supporting assets the disruption of which could cause material harm to the customers or to the continued operation or viability of the BSFI and/or its role in the financial system. Supporting assets refer to people, technology, information, and facilities necessary for the delivery of critical operations. These may include internal process, IT systems, clearing and settlement facilities and outsourced services necessary for the delivery of critical operations, among others. Determining whether a particular operation is "critical" depends on the nature of operations of the BSFI and its role in the financial system.

c. *Critical functions* refer to activities performed for third parties, including external customers, where failure would lead to the disruption of services that are vital for the BSFI's viability, the functioning of the economy or for financial stability due to the BSFI's systemic importance, size or market share, external and internal interconnectedness, complexity, and cross-border activities. Examples include servicing of withdrawals, payments, custody, certain lending and deposit taking activities, clearing and settling.[4]

d. *Operational disruption* is an event or occurrence that impedes the continuous delivery of critical operations. It can be due to man-made causes, such as cyberattacks, social engineering schemes, terrorist threats or attacks, insider abuse or fraud, or natural causes, such as earthquake, typhoon, or tsunami.

e. *Tolerance for disruption* is the maximum level of disruption on the BSFI's critical operations arising from any type of operational risk events or hazards that the BSFI is willing to accept considering a range of severe but plausible scenarios. In determining this, it is important to consider the first point at which disruption to critical operations would cause material harm to customers or risk to market integrity and financial stability. A BSFI's tolerance for disruption is applied at the critical operations level.

f. *Material entities* shall refer, at a minimum, to the bank's/QB's subsidiaries and affiliates, as defined under Section 131/131-Q[5] (Definition of Terms), which represent a significant portion of the balance sheet or business activities of the parent bank/QB.

g. *Service providers* include third parties, intragroup entities (i.e. entities within a group such as parent, subsidiary or affiliate companies) and (if

[3] Largely drawn from the March 2021 Basel Committee on Banking Supervision Principles for Operational Resilience.

[4] Financial Stability Board (FSB) Recovery and Resolution planning for systemically important financial institutions, guidance on identification of critical functions and critical shared services, July 2013

[5] For pawnshops, please refer to Section 105-P (Registered/Business Name.)

applicable) other parties further along the supply chain[6]. This includes providers of outsourced services.

Operational Resilience and its Interaction with Related Processes[7]

a. *Operational resilience* is an end state or outcome wherein the BSFI demonstrates that it can continue to render its critical operations through significant disruption, reducing the impact on its customers and the financial system. This contributes to reinforcing the BSFI's viability amidst significant disruptions, promoting the financial system's resilience and stability and servicing the real economy. Critical to achieving this is the recognition that disruptions will occur, necessitating forward looking assessments, including emerging risks, as well as careful planning and preparation to respond accordingly, as part of the BSFI's overall risk management. Operational resilience, therefore, is not a stand-alone objective. Rather, it needs to be integrated with the BSFI's governance structures and other related risk management processes, such as operational risk, business continuity, information and communications technology (ICT) including cybersecurity, third party risk, and recovery plans.

b. *Operational Risk Management*[8]. The operational resilience framework is intricately linked to the operational risk management function. While operational risk pertains to the risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events, operational resilience views the impact of these individual factors on the ability of a BSFI to continuously deliver its critical operations. Operational resilience goes beyond reducing the likelihood of occurrence of operational risk events or the amount of operational loss that may be suffered by the BSFI. While operational risk management focuses on the losses that may be caused to the BSFI, operational resilience considers the impact of disruptions to critical operations or the harm that failure to deliver critical operations may cause not only to the BSFI but to its customers and the wider financial system.

c. *Business Continuity Management[9](BCM)* is an essential component of operational resilience. Both support the continuous business operations when unexpected events occur. BCM focuses on individual points of failure while operational resilience complements this by looking into the end-to-end delivery of critical operations. The crisis management framework, as part of BCM, is activated or triggered during disruptive events. Meanwhile, the operational resilience framework covers an expansive set of capabilities, including crisis management, to achieve resilience across a broad range of disruptions.

d. *Cybersecurity*[10]. Cybersecurity refers to technologies, processes, and practices designed to protect the BSFI's information assets and consumers, including third parties, by preventing, detecting, responding to and recovering from cyber-attacks. BSFIs should continually assess cyber-related attacks and incidents relative to their computing environment and understand the evolving cyber threat landscape to institute appropriate

[6] Basel Committee on Banking Supervision, Core principles for effective banking supervision, April 2024
[7] The Bangko Sentral's Operational Resilience Guidelines complement the existing policies in the Manual of Regulations on Operational Risk Management, Business Continuity Management, IT Risk Management, Cybersecurity, and Outsourcing Framework.
[8] Section 146/146-Q. For other NBFIs, please refer to Section 125-N/163-T, as applicable.
[9] Section 149/148-Q. For other NBFIs, please refer to Section 146-S/143-P/127-N/164-T, as applicable
[10] Section 148/147-Q. For other NBFIs, please refer to Section 145-S/142-P/126-N, as applicable.

cyber resilience capabilities. A strong cybersecurity program allows for detection of risks to operational resilience, influences cyber security priorities, and enhances cyber resilience. An effective resilience approach, which includes identifying critical operations and tolerance for disruption and considering the threat landscape, is essential in supporting and achieving the BSFI's operational resilience.

e. *Third Party Risk Management*[11]. Over the years, BSFIs have made increasing use of third-party service providers in the delivery of financial services, including those that are integral to critical operations. While the use of third-party service providers enables BSFIs to benefit from available expertise and synergies, this has contributed to heightened complexity and may reduce oversight over potential vulnerabilities in the delivery of critical operations. BSFIs should ensure that third-party service providers for processes that feed into their critical operations have at least the equivalent level of operational resilience as established by the BSFI during "business as usual scenarios" and in the event of disruption. The principles on outsourcing arrangements shall apply to third party risk management for operational resilience purposes.

Key Elements of Operational Resilience

a. **Utilize existing governance structure to establish, oversee, and implement an effective operational resilience approach.** Governance structure covers the roles and responsibilities of the board of directors and senior management on the various stages of operational resilience, starting from development up to approval, implementation, and ongoing review or enhancement of the operational resilience framework. The board of directors shall be primarily responsible for the oversight and approval of the operational resilience framework as well as the roles of the three-lines of defense for operational resilience. It shall ensure that the first line or the business units and internal controls, the second line or the risk management function and compliance, and the third-line or the internal audit, adhere to the principles of operational resilience. Meanwhile, the senior management shall take the lead in implementing the operational resilience framework, assessing the BSFI's operational resilience capability, and communicating the necessary remedial actions to the board of directors.

b. **Determine critical operations, tolerance for disruption, and severe but plausible scenarios.** The basic building blocks of operational resilience include the initial steps of identifying the BSFI's critical operations, setting of tolerance for disruption and determining the range of severe but plausible scenarios, of varying nature, seriousness, and duration relevant to its business and risk profile. These are essential in prioritizing critical operations and determining capabilities to withstand and absorb disruption within the tolerance level acceptable to the BSFI, considering the range of adverse scenarios identified.

c. **Map interconnections and interdependencies.** Understanding the operations, interconnections and interdependencies allows BSFIs to identify and resolve vulnerabilities that exist in the delivery of critical operations. BSFIs should map the chain of activities in the delivery of critical operations, especially those arising from the network of

[11] Section 112/111-Q. For other NBFIs, please refer to Section 113-S/112-P/102-N/112-T, as applicable. Section 148/147-Q. For other NBFIs, please refer to Sec. 145-S/142-P/126-N, as applicable.

interconnections and interdependencies and those that are performed by service providers. This will enable the BSFIs to holistically assess the sources of vulnerabilities and invest in appropriate resilience measures before disruption occurs so that BSFIs can remain within their tolerance for disruption. It also complements the development of severe but plausible scenarios that point to vulnerabilities along the processes involved.

d. **Plan and manage risks to critical operations.** After identifying critical operations and the related interconnections/interdependencies, it is equally important to plan for and manage the material and/or emerging risks or events that will hamper the continuous delivery of critical operations to the customers and affect the BSFI and financial system. This is not a silo approach but rather necessitates leveraging on existing and working relevant risk management frameworks of the BSFI, for an integrated and enterprise-wide approach to managing risks associated with the delivery of critical operations. In this regard, BSFIs are expected to consider risk management components with nexus to operational resilience such as operational risk, business continuity, third party risk, and information and technology risk.

e. **Test ability to deliver critical operations amidst disruption under severe but plausible scenarios.** Operational resilience builds on the continuous process of business continuity management and periodic testing exercises to gauge the BSFI's ability to deliver critical operations through a range of severe but plausible scenarios. Recognizing that disruptions will occur, the BSFI must make an exhaustive and informed identification of disruptive events and incidents, of varying degrees, nature, duration, and plausibility, that may affect the delivery of its critical operations. This should also encompass the identified interconnections and interdependencies, both internal and external. The periodic testing exercise should sharpen the personnel's operational resilience awareness and its results should inform refinements in the operational resilience framework.

f. **Respond and recover from disruption.** When a disruption occurs affecting the BSFI's critical operations, the BSFI should have the ability to respond, manage and deliver critical operations consistent with its integrated operational resilience framework. This should include, among others, clear delineation of the roles and responsibilities and succession of authority in the event of disruption; and an incident response plan that contains key steps to handle the disruption and assess how it will affect the BSFI's risk appetite and tolerance for disruptions. As part of its incident response plan and to strengthen its response capabilities, the BSFI should maintain a catalogue that includes an inventory of incident response and recovery actions, roles and responsibilities of key officers/personnel as well as internal and external resources. The incident response plan should capture the life cycle of an incident, classification of events or disruptions based on severity, response and recovery procedures and communication plan. Also, it should be periodically tested, reviewed and updated.

g. **Review, refine and update risk management and operational resilience framework.** Operational resilience should be integrated with the BSFI's overall enterprise-wide risk management approach. Maintaining operational resilience posture is a continuous activity. Accordingly, the operational resilience framework must be dynamic and periodically reviewed, refined and updated to remain in line with the BSFI's risk appetite, tolerance for disruption, business model and complexity, among

others. Reviews should be conducted regularly or when necessary (e.g., when there are material changes in the operations or business activities of the BSFI).

More detailed guidelines on each of these elements are outlined in *Appendix 158/Q-102.*

Reporting and Notification Requirements. BSFIs shall disclose in their Annual Report the overarching approach to operational resilience. This includes providing an overview of the operational resilience approach and key information on the operational resilience components. Moreover, the BSFI shall inform the appropriate supervising department of the Bangko Sentral within twenty-four (24) hours from activation of the incident response plan for critical operations. The notification shall indicate the following information, among others, as applicable:

a. Nature, duration and root cause of the disruption;
b. Affected critical operations and impact of the disruption on the delivery of critical operations;
c. Status if tolerance for disruption is breached; and
d. Actions that have been taken and/or intended to be taken by the Management to continue delivery of the critical operations.

The report may contain initial information available as of the reporting timeline. The Bangko Sentral may request additional information it deems warranted.

If the incident also qualifies for event-driven reporting under Section 148/147-Q[12], there is no need to file a separate report as required in this Section. Meanwhile, operational risk events which are covered by the report prescribed in this Section shall no longer require a separate reporting under Section 146/146-Q[13]. However, submission of the incident report required herein shall not excuse the BSFI from complying with the existing regulations on reporting of crimes and losses under Section 173/172-Q[14].

Supervisory *Review by the Bangko Sentral.* The Bangko Sentral shall review the operational resilience framework of the BSFI as part of the overall supervisory process, focusing on assessing the robustness, credibility, and feasibility of delivering critical operations through disruption and within the BSFI's defined tolerance for disruption.

Supervisory *enforcement actions.* Consistent with the provisions of Section 002/002-Q[15], the Bangko Sentral may deploy appropriate supervisory enforcement actions to promote adherence with the requirements set forth in this Section and bring about timely remedial actions.

Section 2. Sections 142-S/125-N/163-T of the MORNBFI shall be revised and Section 131-CC shall be added in the MORNBFI, as follows:

"Section 142-S RISK MANAGEMENT FUNCTION

---

[12] For other NBFIs, please refer to Sections 145-S/142-P/126-N (Reporting and Notification Standards), as applicable
[13] For other NBFIs, please refer to Sections 125-N/163-T (Notification/ Reporting to Bangko Sentral), as applicable
[14] For other NBFIs, please refer to Sections 162-S/161-P/901-N/183-T (Report on crimes/losses), as applicable
[15] For other NBFIs, please refer to Sections 002-S/002-P/001-N/002-T, as applicable

xxx

Chief Risk Officer (CRO). xxx

xxx

Operational Resilience. *The provisions of Section 146-Q and Appendix Q-102 on Operational Resilience guidelines shall govern non-stock savings and loan associations to the extent applicable."*

"Section 125-N/163-T OPERATIONAL RISK MANAGEMENT AND OPERATIONAL RESILIENCE

xxx

Supervisory Enforcement Actions. xxx

Operational Resilience. *The provisions of Section 146-Q and Appendix Q-102 on Operational Resilience guidelines shall govern other non-bank financial institutions/trust corporations to the extent applicable."*

"Section 131-CC Operational Resilience

The provisions of Section 146-Q and Appendix Q-102 on Operational Resilience guidelines shall govern non-bank credit card issuers to the extent applicable."

Section 3. Transitory Provisions. The following provisions on the phased implementation of the requirements of this Circular shall be incorporated as a footnote to Section 146 of the MORB and Section 146-Q of the MORNBFI on Item II: Guidelines on Operational Resilience:

a. Phase 1- Within one (1) year from the effectivity of the Circular – All BSFIs shall submit to the appropriate supervising department of the Bangko Sentral an accomplished Self-Assessment Questionnaire (Annex A) comprised of a gap analysis and action plans to comply with the requirements of this Section.

b. Phase 2 – Within two (2) years from the effectivity of the Circular – All universal, commercial and digital banks and complex non-bank BSFIs specifically identified by the supervising department based on their systemic importance, shall have developed and/or integrated the operational resilience framework within their existing risk management systems, with due consideration of the applicable requirements in this Section. Disclosure of key elements of operational resilience in the Annual Report shall commence after Phase 2.

c. Phase 3 – Within three (3) years from the effectivity of the Circular – All thrift and rural/cooperative banks and other BSFIs shall have developed and/or integrated the operational resilience framework with their existing risk management systems, with due consideration of the applicable requirements in this Section. Disclosure of key elements of operational resilience in the Annual Report shall commence after Phase 3.

Section 4. Section 175 of the MORB, as amended by Circular No. 1186 dated 21 December 2023, and 174-Q of the MORNBFI on disclosure requirements in the annual report, are hereby amended to read, as follows:

"175 DISCLOSURES TO THE PUBLIC

xxx

Disclosure requirements in the annual report. xxx

xxx

All banks shall prepare an annual report which shall include a discussion and/or analysis of the following minimum information in no particular order:

xxx
g. Audited financial statements (AFS). xxx;
h. information on sustainable finance as required under Sec. 153; and
i. information on the operational resilience approach as required under Section 146.

xxx

"174-Q PUBLIC DISCLOSURES

Disclosure requirements in the annual report. xxx

xxx

All QBs shall prepare an annual report which shall include, in addition to the AFS and other usual information contained therein, a discussion and/or analysis of the following minimum information in no particular order:

xxx
g. Corporate information;
h. Audited financial statements (AFS); and
i. information on the operational resilience approach as required under Section 146-Q.

Section 5. Effectivity. This Circular shall take effect fifteen (15) calendar days following its publication either in the Official Gazette or in a newspaper of general circulation.

FOR THE MONETARY BOARD:

BERNADETTE ROMULO-PUYAT
Officer-in-Charge

28 October 2024

Appendix *158/Q-102*

OPERATIONAL RESILIENCE GUIDELINES
(Appendix to Section 146/146-Q)

I. Governance Structure

1. The board of directors shall be primarily responsible for the oversight and approval of the operational resilience framework that enables the BSFI to identify and prepare for, respond and adapt to, and recover and learn from operational disruptions.

    a. Operational resilience framework shall be aligned with the overall governance and risk management system of the BSFI. In this regard, the existing governance frameworks and committees that exercise oversight on related areas shall consider operational resilience in their business objectives and strategies in the lens of critical operations.

    b. For a holistic approach, the development of operational resilience framework should leverage other related elements of risk management, such as operational risk, business continuity, third party risk, and ICT and cybersecurity risk, as applicable. A clear mechanism for coordination and collaboration shall be established between and among these relevant functions to strengthen the BSFIs operational resilience.

    c. The operational resilience framework shall clearly communicate and promote understanding of the relevant internal and external parties' roles and responsibilities with respect to the overall operational resilience approach and objectives.

2. The senior management shall implement the operational resilience framework and ensure efficient and effective allocation of resources and capabilities for this purpose.

3. The senior management shall be responsible for ensuring the conduct of an overall assessment of the BSFI's operational resilience capability and periodic reporting to the board of directors/board-committee. This will allow the board of directors to assess the BSFI's capabilities to remain within its set tolerance and deliver critical operations through disruptions. The board of directors shall periodically review and continuously gain sufficient understanding of the BSFI's operational resilience profile and capabilities through senior management's information and reports.

4. The senior management shall implement remedial actions necessary to ensure that resources and capabilities to remain operationally resilient are timely communicated to the board of directors. This will aid in the decision-making by prioritizing activities or target investments that will help improve operational resilience or focus on critical operations which will have the most significant impact when disrupted.

5. The board of directors shall oversee the three lines of defense for operational resilience and ensure that these functions are operating as intended:

a. The first line is responsible for ensuring that all the resources needed in the end-to-end delivery of critical operations are identified. This should include those provided by a third-party and in certain cases, those that are sourced by the third-party from other service providers. The first line also ensures that risk exposures are aligned with the established tolerance for disruption for each critical operation. The first line shall ensure that material operational resilience-related information (e.g. loss events, incidents, et.al) are adequately and timely escalated to senior management/board of directors and communicated to the relevant independent control functions.

b. The second line is expected to assess the end-to-end activities of critical operations and their extent of exposure to operational disruptions. It should conduct periodic review to ensure that internal controls are in place for critical operations and continue to adapt to the changing environment. It should also ensure that risk exposures of the resources for critical operations are well managed to allow critical operations to remain within the tolerance for disruption.

c. The third line assesses the design and ongoing effectiveness of the BSFI's operational resilience efforts. It should challenge the first and second lines on the appropriateness of the resources for critical operations to operate within the tolerance for disruption.

II. Key Elements of Operational Resilience

1. Determine critical operations, tolerance for disruption and severe but plausible scenarios

   a. Identifying critical operations

      i. *Criteria for identification of critical operations.* BSFIs should have a board-approved criteria for identifying and prioritizing critical operations. The approach in determining critical operations may vary across the BSFIs but shall consider relevant factors, such as the impact of a disruption on the operations to the BSFI's viability, its customers, or its role in the financial system. The identification process should cover the end-to-end activities necessary in delivering critical operations, rather than the individual people, process, or system.

      ii. The BSFI may take into account the business outcome approach to prioritize activities or services that when disrupted will pose material risks to its viability, or systemic risk to the financial system, as well as disadvantages to the customers and other stakeholders. Rather than focusing on a specific process or system of the BSFI, operational resilience entails protecting its critical operations to ensure continuous delivery throughout disruption. BSFIs should also leverage or consider existing identification and classification of key functions or services in determining critical operations, such as those identified in the recovery plan[16]. The number of identified critical operations should be commensurate with the BSFI's size, nature, and complexity of operations.

[16] Guidelines on Recovery Plans of Banks under Section 156 (Circular No. 1158 dated 18 October 2022)

iii. *Identified critical operations.* The Board should approve the identified critical operations which should be proportionate to the nature, scale, and complexity of the BSFI's business. The identified critical operations will drive the subsequent steps of setting tolerance for disruption and mapping of interconnections and interdependencies, among others.

iv. Operational risk management function shall be utilized to identify and assess vulnerabilities, and manage, to the extent possible, the operational risks affecting critical operations. BSFIs may also leverage other frameworks to establish linkage or distinction of critical operations with respect to operational resilience vis-a-vis business continuity management and recovery planning, among others.

The identification process should be dynamic and take into account changes in the elements of critical operations, lessons learned from disruptions and new threats or vulnerabilities. The propriety and effectiveness of this process should be periodically assessed.

b. Setting the tolerance for disruption

i. BSFIs shall set the tolerance for disruption on each identified critical operation. In the context of operational resilience, a disruption is assumed to occur given various severe but plausible scenarios. For this reason, tolerance for disruption shall be set as the maximum level of disruption that the BSFI is willing to accept on its critical operations.

ii. In establishing clearly defined tolerance for disruption, BSFIs shall consider either or both quantitative and qualitative metrics. This shall include, at a minimum, a time-based metric which generally sets the acceptable timeframe or schedule that BSFIs will be able to restore the delivery of critical operations before it could pose material risk to the BSFI and identified external stakeholders. Other metrics shall be considered, such as the maximum number of customers or volume and value of transactions affected by the disruption. BSFIs may also leverage other metrics utilized in existing frameworks and expound or link, as necessary with the delivery of critical operations. Tolerance for disruption should be tested against severe but plausible scenarios to determine its relevance and propriety.

iii. Tolerance for disruption shall aid the BSFIs in assessing its overall resiliency capabilities and drive improvements to strengthen operational resilience, particularly when tolerance is breached upon testing.

iv. The criteria on the elements of operational resilience, particularly on the (a) identification of critical operations, and (b) setting of tolerance for disruption shall be reviewed, challenged, and approved by the board of directors. A mechanism should be in place to keep the criteria responsive to changes and significant developments in

the business environment, in line with existing change management process[17].

c. Determining severe but plausible scenarios.

i. A robust operational resilience framework entails identifying a broad array of severe but plausible scenarios, of varying nature, degree, and duration, relevant to the BSFI's idiosyncratic risk profile and operations, and their impact on the delivery of the BSFI's identified critical operations. The scenarios must be informed by realistic assumptions distinct to the BSFI, its business, and its internal and external operating environment.

ii. Examples of scenarios that BSFIs are strongly encouraged to consider include the "Big One" or the worst-case scenario should the West Valley Fault move and generate a magnitude of 7.2 quake, severe typhoon, failure of critical third-party service provider, disturbances in payment and settlement systems, and a simultaneous or coordinated cyberattack/ransomware on a number of banks.

2. Map interconnections and interdependencies

a. BSFIs should have an adequate understanding of how each of its critical operations is being delivered. The BSFI should perform an end-to-end mapping of the starting point from how the critical operation is activated up to the ultimate delivery of the service to its client. A critical operation may also involve a continuing process or iteration.

b. BSFIs should be able to identify key resources to keep each critical operation running even in times of disruptions. These may include, but not limited to, people, processes, technology and information facilities, and other resources including those under third-party service arrangements.

c. Mapping should extensively identify interconnections and interdependencies of the resources needed. Doing this would allow determination of possible stress or friction points within the chain, including the impact on the use of common resources within the BSFI or even those that are external to the BSFI under certain arrangements. An acceptable mapping should identify vulnerability points and support the established tolerance for disruption for each critical operation.

d. When a third-party service provider is involved in the delivery of critical operations, the BSFI should have an adequate understanding of the extent of the role of the service provider, including the interdependencies of other processes to the provider. The BSFI should be aware of arrangements where the service provider further engages other providers that may impact the provision of a critical operation.

[17] A bank's operational risk exposure evolves when it initiates change, such as engaging in new activities or developing new products or services; entering into unfamiliar markets or jurisdictions; implementing new business processes or technology systems or modifying existing ones; and/or engaging in businesses that are geographically distant from the head office. Change management should assess the evolution of associated risks across time throughout the full life cycle of a product or service.; Basel Committee on Banking Supervision, Core principles for effective banking supervision, April 2024

Identification of these interconnections and interdependencies in the delivery of critical operations should inform, among others, the development of severe but plausible scenarios.

e. Mapping exercise for operational resilience should be harmonized with the related activities in other risk management functions such as those in operational risk, third party risk, business continuity and ICT risk.

3. Plan for and manage risks to delivery of critical operations

a. Planning is critical to the BSFI's ability to manage all material and/or emerging risks or events that will affect the continuous delivery of critical operations to mitigate impact on the customers, on the BSFI and the financial system. This is not a silo approach but rather necessitates leveraging existing and working relevant risk management frameworks of the BSFI, for a holistic and integrated approach to managing risks associated with the delivery of critical operations. In this regard, BSFIs are expected to consider risk management components with nexus to operational resilience.

b. BSFIs should utilize their operational risk management processes to continuously assess the external and internal threats, possible breakdowns in controls, processes, and systems, as well as vulnerabilities in critical operations and manage identified risks to critical operations. The operational risk management function should work with relevant functions to mitigate risks that will hamper the delivery of critical operations. There should be periodic assessment of the adequacy of controls and procedures, particularly those affecting critical operations, including in cases of changes to the underlying components of the critical operations, to consider lessons learned from disruptive events or to account for new threats and vulnerabilities.

c. BSFIs should utilize existing change management capabilities in line with the existing change management processes to assess potential effects on the delivery of critical operations and on their interconnections and interdependencies. The BSFI's change management process should be comprehensive, appropriately resourced, and adequately divided up between the relevant lines of defense.

d. When a third-party service provider is involved, the BSFI should conduct due diligence to ensure that the service provider aligns with the operational resilience framework of the BSFI. In the same manner, the BSFI should be satisfied that the service provider conducts its own mapping process and supports the established tolerance for disruption. It should also consider the possible concentration of services to a limited number of service providers. No arrangement should be entered into when the service provider cannot comply with the tolerance for disruption as assessed during the conduct of due diligence.

e. Third-party service arrangements which impact critical operations must contain details of how critical operations should be maintained or serviced during disruptions or an exit strategy in case the service provider is not able to deliver the service. The BSFI should identify alternative arrangements including identifying substitutes or even performing the service back within the BSFI.

f. Dependencies on public infrastructure, such as telecommunications, transportation, and energy, should be assessed in terms of its impact on the BSFIs' critical operations and established tolerance for disruption.

g. The BSFI's technology and security are critical in maintaining a safe and resilient operating environment. Therefore, BSFIs should adopt risk-based strategies responsive to the evolving threat landscape that employ an integrated and multi-layer approach, ensuring the critical operations' IT environment and information confidentiality, integrity, and availability through disruptive events. The BSFI should ensure that these strategies have adequate authentication, authorization, and auditing controls to maintain the security of the critical operations' IT environment. The BSFI should also ensure that ICT protection, detection, response and recovery processes are regularly tested following an increasing complexity, considering severe but plausible scenarios, and relevant information are timely conveyed for risk management and decision-making processes to support and facilitate the delivery of critical operations. Likewise, the BSFI should evaluate the extent of its interconnections[18] and implement appropriate risk mitigation measures to achieve its operational resilience goals and contribute towards improving the entire ecosystem.

4. Test ability to deliver critical operations amidst disruption under severe but plausible scenarios.

   a. The BCM, including the business continuity plan (BCP), should be integrated into the operational resilience framework, in line with the BSFI's overall risk appetite and tolerance for disruption. A forward-looking BCM that assesses the impact of potential disruptions on critical operations must be in place. In line with this, the BCM should cover the following:

      i. Business impact analyses and recovery strategies, as well as testing, awareness and training programmes;
      ii. Bespoke and detailed guidance on the implementation of the incident recovery plan for critical operations, including defining the triggers for invoking the BCM, outlining the roles and responsibilities for managing operational disruptions, providing clear cut rules on succession of authority in case of disruptions affecting key personnel, and the internal decision-making process; and
      iii. Communication and crisis management programs.

   b. Periodic business continuity exercises, encompassing the identified critical operations and their interconnections and key dependencies, must be in place, using a range of severe but plausible scenarios. The scenarios must be informed by realistic assumptions distinct to the BSFI and its operating environment, considering disruptive events and incidents of varying degrees, nature, duration, and plausibility, that may affect the delivery of its critical operations. This may include pandemic, natural calamities, failure of key service providers, and major cyber incidents. The BSFI may consider its own experiences or across the sector, or even cross-sectoral, as applicable, given the operating landscape. The BSFI can also leverage the identified scenarios in its

[18] Appendix 75/Q-62

existing risk management framework and expand the same to consider operational resilience aspects.

c. The BSFI shall employ a suitable mix of manner of testing exercises (e.g., tabletop, simulations or live testing) depending on their characteristics, objectives and benefits. It should also account for and manage the risks arising from the conduct of testing. The timing and frequency of testing should be informed by a range of relevant factors, such as the number of identified critical operations, significant changes in the BSFI's operating environment or nature and severity of identified disruptions, and impact of the disruption.

d. Competent and relevant personnel should be involved in the testing. The manner of testing will also drive, in part, the personnel, position and function required to be part of the exercise.

e. The BSFI should consider that the business continuity testing should, among others, heighten the personnel's operational resilience knowledge and readiness to effectively adapt and respond to disruptions. The testing may disclose a vulnerability in one process or function related to the critical operations, which may require remediation efforts, such as identifying alternative channel or substitute, process or system enhancement or staff training. The testing may also disclose a scenario where there is a breach of set level of tolerance, which warrants board and senior management action. The results of the testing exercise must be documented and reported to the board. It must include, among others, the observed gaps or weaknesses as well as the adjustments made or needed to achieve operational resilience. The results of the testing exercise should also inform refinements or enhancements in the operational resilience framework, as appropriate.

f. BSFIs may leverage and/or enhance its existing BCM, disaster recovery and/or recovery and resolution plans to capture operational resilience principles and enable it to deliver critical operations through disruptions.

5. Respond to and recover from disruptive events

a. BSFIs should acknowledge that disruptions will occur underscoring the importance of planning and testing their ability to deliver critical operations through disruption. This requires a change in perspective towards operational disruptions from a probabilistic approach to an expectation that it will happen.

b. When a disruption occurs affecting the BSFI's critical operations, the incident response plan should be activated. It should capture the life cycle of a disruption, contain key steps to handle the disruption to ensure delivery of critical operations and assess how it will affect the BSFI's risk appetite and tolerance for disruptions. It should also clearly delineate the roles and responsibilities and succession of authority during the disruption. Key officers and personnel should be identified and/or designated who will decide and implement actions to ensure delivery of critical operations through disruptions.

c. BSFIs should identify the full range of recovery options to enable critical operations to be maintained or restored within tolerance for disruption.

As part of its incident response plan, the BSFI should maintain a catalogue to support its response capabilities, such as key officers and personnel, internal and external resources that may be affected, response and recovery procedures, and communication plan.

d. Communication plan is a critical part of the operational resilience framework and incident management. An incident communication plan, with internal and external communication matrix, should be developed to ensure effective, timely and targeted communications during a disruption. This will ensure proper escalation and flow of information, decisions, and updates to stakeholders concerned. Key resources and experts to serve as focal spokesperson/s during disruptions should be identified for effective communication strategy.

e. Operational risk tools such as, but not limited to, loss events database should capture incidents that have the potential to disrupt the delivery of critical operations. For operational resilience, these incidents should be further examined to cover its full life cycle, from classification of incidents severity to response and recovery procedures, communication plans and root cause analysis to reflect lessons learned.

f. The incident response plan should be periodically reviewed, tested, and updated, including lessons learned from previous disruptions.

6. Review, refine and update risk management and operational resilience framework.

Achieving operational resilience is a dynamic process. As such, learnings from experiences are critical to the continuous reinforcement of the BSFI's operational resilience approach. After experiencing and recovering from a disruption, a stocktaking of lessons learned will enable the BSFI to reflect on the key components of its operational resilience framework, the actions and decisions made, as well as identifying what has worked and what failed. This will be useful inputs to refining the operational resilience framework and its key elements, considering among others, reflections on the following:

a. Root cause of the disruption and the vulnerability/ies exploited;
b. Impact on the delivery of affected critical operations;
c. Adequacy of controls, actions, and decisions made;
d. Duration of disruption until resumption of critical operations and if set tolerance for disruption remains; and
e. Necessary adjustments, if any, to remediate the gaps identified.

BSFIs are required to periodically review, refine, and update the operational resilience framework to ensure that it is aligned with their risk appetite, tolerance for disruption, business model and complexity, among others. Other events that could trigger review and/or refinements in the framework include material changes in its business and operating environment, critical operations, and tolerance for disruptions.

Annex A

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Objectives of the Self-Assessment Questionnaire (SAQ)

1. To provide an overview of the BSP-supervised financial institutions (BSFI)'s operational resilience capabilities and highlight priority areas for development; and

2. To support the board of directors (board) and senior management, and the bank supervisors' understanding of the BSFI's operational resilience capabilities and readiness as well as capture the BSFI's journey to achieving operational resilience.

Timeline

One year from the effectivity of the Circular – All BSFIs shall submit to the appropriate supervising department a transition plan using the SAQ comprised of a gap analysis and action plans to achieve operational resilience.

Part I. Gap Analysis

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
A. Governance Structure	• Has the BSFI identified a board-level Committee in-charge of overseeing the integration of operational resilience principles with its existing risk management framework? • Has the BSFI articulated the roles and responsibilities of the board and senior management for operational resilience?			

[1] This does not cover all the minimum considerations but suggestions of what may be looked into.
[2] Provide brief and concise description of the BSFI's compliance (e.g., process or policy applicable to the requirement)
[3] Provide the key action plans, responsible unit/officer and timeline to achieve the requirement for operational resilience purposes

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	• Has the BSFI defined the roles of the business units, compliance, risk management function, and internal audit for operational resilience? • Has the BSFI identified changes, if any, that will be made in the existing bank guidelines/processes (e.g., operational risk management, business continuity, outsourcing/third-party risk management) in order to align or integrate with the operational resilience approach? • Has the BSFI identified material entities for a group-wide operational resilience framework? • For foreign bank branches – Has the head office adopted an operational resilience framework? Is it being implemented for the Philippine Branch? • Has the board approved the BSFI's operational resilience framework? • Has the board discussed how the BSFI would respond if operational disruptions occurred?			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	• Has the board reviewed and approved the identified critical operations, tolerance for disruption and range of severe but plausible scenarios?			
B. Key Elements of Operational Resilience				
1. Determine critical operations, tolerance for disruption and severe but plausible scenarios a. Identifying critical operations	• Has the BSFI identified its critical operations? Did the Board approve the identified critical operations? • How did the BSFI identify its critical operations? Please provide the criteria used, assumptions, and justifications on why said operations have been identified as critical. • Are there any changes in the business model, processes or activities after identifying critical operations (e.g., resource allocation)?			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
b. Setting the tolerance for disruption	• Has the BSFI set the tolerance for disruption and has it been approved by the Board? • Has the BSFI developed a methodology or criteria in setting tolerance for disruption? • Has the BSFI assigned personnel/unit(s) that are responsible for monitoring that the BSFI is operating within its tolerance of disruption? • Is there a reporting mechanism to notify the BSP in case the BSFI activated the incident response plan?			
c. Determining severe but plausible scenarios.	• Has the BSFI identified scenarios that would directly impact its critical operations? Are these considered as severe and plausible scenarios? Why? • Has the BSFI documented the basis for the severity of the scenarios? • Has the BSFI considered among its scenarios the "Big One", severe typhoon, failure of critical third-party service provider, disturbances in payment and settlement systems, and a simultaneous or			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	coordinated cyberattack/ransomware on a number of banks?			
2. Map interconnections and interdependencies	• Has the BSFI identified the personnel primarily responsible for overseeing and conducting the mapping of activities involving critical operations? • Has the BSFI mapped/identified the interconnections and interdependencies involving critical operations? If no, when is the expected timeline to complete the mapping/identification process? • What are the key sources and resources used to support the BSFI's mapping? • Has the BSFI identified the key roles that support the delivery of critical operations and established the plans in case of unavailability of the individuals fulfilling these key roles? • Are there third-party service providers involved in the delivery of critical operations? Does the BSFI set the requirements and coordinate with the service provider regarding its expectations for operational resilience to ensure delivery of critical operations through disruption?			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	• Has the BSFI identified any vulnerabilities in its mapping exercise? What are the vulnerabilities identified? Are action plans adopted or implemented to resolve such vulnerabilities? • How will the mapping be kept up to date? Who is responsible for and what is the frequency of review/updating to ensure that it remains relevant and reflective of the BSFI's tolerance for disruption and critical operations?			
3. Plan for and manage risks to delivery of critical operations	• Has the BSFI identified disruptions and vulnerabilities that may impact critical operations? • Are the identified disruptions or vulnerabilities affecting only one or more than one critical operation? • Based on the identified disruptions and vulnerabilities, are there sufficient plans, processes, and resources to ensure delivery of critical operations throughout the disruptive events? What are the changes made to ensure delivery of critical operations throughout the disruptions?			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	• What vulnerabilities still exist that have not yet been remediated or where the Board has accepted a risk level? • What vulnerabilities might arise from reliance on third-party services, if any? Are action plans adopted or implemented to address those vulnerabilities to support operational resilience? • Is there a periodic assessment of adequacy of controls and procedures affecting critical operations, including in cases of changes to its underlying components? • Is there a change management process? Are existing change management capabilities utilized to assess potential effects on delivery of critical operations and their interconnections/inter-dependencies? Is the change management process comprehensive, appropriately resourced, and adequately divided up between the relevant lines of defense? • Has the BSFI adopted strategies to ensure the critical operations' information technology environment and information confidentiality, integrity, and availability through disruptive events?			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	• Has the BSFI assessed the substitutability of critical third parties, including the option to revert to in-house units in cases of failure with third-party dependencies?			
4. Business Continuity Management (BCM) and Testing	• Is the BCM integrated into the operational resilience framework? • Has the BSFI covered the identified critical operations and defined tolerance for disruptions in its BCM and testing? If yes, what are the key changes made, if any. If no, how does the BSFI plan to incorporate these in its BCM to achieve operational resilience? • Does the BCM consider the impact of potential disruptions on critical operations given the set tolerance for disruption? • Does the BCM cover the critical elements, such as business impact analyses, incident response and recovery plan and communication plan, to support delivery of critical operations through disruptions and to keep the same within the tolerance level? • Is there a periodic business continuity exercise based on a range of severe but			

SELF-ASSESSMENT QUESTIONNAIRE ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	plausible scenarios in relation to the critical operations? • What are the identified scenarios and the assumptions used in identifying those events? • Has the BSFI leveraged scenarios identified under existing risk management framework? • What is the manner, timing and frequency of the testing exercise? Who leads this activity? • Has the BSFI tested the ICT protection, detection, response, and recovery processes following an increasing complexity considering severe but plausible scenarios?			
5. Respond to and recover from disruptive events	• How will the response and recovery strategies enable the BSFI to reduce material harm to the customers, BSFI and the financial system, caused by operational disruption on critical operations? • Has the BSFI developed strategies and procedures to mitigate harm caused by			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	operational disruptions to consumers and minimize risk to market integrity? • Has the BSFI developed an incident response plan to ensure delivery of critical operations throughout disruption? Does it cover the life cycle of the disruption, steps to ensure delivery of critical operations as well as the respective roles and responsibilities in its implementation? • Has the BSFI considered succession planning for the key personnel in the incident response plan? • Has the BSFI developed internal and external communications plans in case of disruptions to critical operations? • What is the policy for the periodic review of the incident response plan?			
6. Review, refine and update risk management and operational resilience framework	• Is there a database containing all the incidents or disruptions that affect the critical operations? Does it capture the life cycle of the incident and assess its severity? Does it contain information on the actions taken on these incidents? • Has the BSFI developed a mechanism to regularly review these incidents and			

SELF-ASSESSMENT QUESTIONNAIRE
ON THE OPERATIONAL RESILIENCE FRAMEWORK

Requirements of the Circular	Guide Questions[1]	BSFI's Compliance		
		Fully compliant	Partially/Non-Compliant	
		Details of Compliance[2]	Identified Gaps	Action Plan[3]
	integrate the actions taken on the operational resilience framework and overall enterprise-wide risk management? • Has the BSFI identified who will initiate or lead the review or update of the operational resilience framework? What is the frequency of the review process?			
Additional Questions on the SAQ • What is the governance/approval process for the SAQ? • Which personnel/unit(s) are responsible for preparing the SAQ?		BSFI's Response:		

SELF-ASSESSMENT QUESTIONNAIRE ON THE OPERATIONAL RESILIENCE FRAMEWORK

Part II. Summary

1. **Overview of the BSFI's Operational Resilience Plan**

   Given the identified gaps and action plans, what is the BSFI's holistic transition plan in adopting an operational resilience framework? What are the key vulnerabilities/gaps identified, and what is the BSFI's timeline to remediate this to achieve operational resilience?

2. **Strategies**

   What are the key strategies to become operationally resilient?

3. **Challenges Encountered**

   What are the challenges/limitations encountered in the adoption and/or execution of the BSFI's operational resilience framework?

   What are the key strategies of the BSFI to address these challenges and achieve operational resilience?

4. **Board Approval**

   Provide details of Board approval on the accomplishment of the SAQ.

5. **Remarks**

   This portion may also be used to provide additional information.