Discussion Paper

(Provisional Translation)

Discussion Paper on Ensuring Operational Resilience

April 2023

Financial Services Agency

Table of Contents

List of boxes

I. Introduction

1. Why does operational resilience matter?

The business environment surrounding financial institutions is changing rapidly. The risk environment is becoming more complex due to a multiple of factors including increased dependence on IT systems, large-scale technology failures, pandemics, growing threats to cybersecurity, the widespread use of cloud services, and burgeoning interdependence through collaboration with FinTech companies.

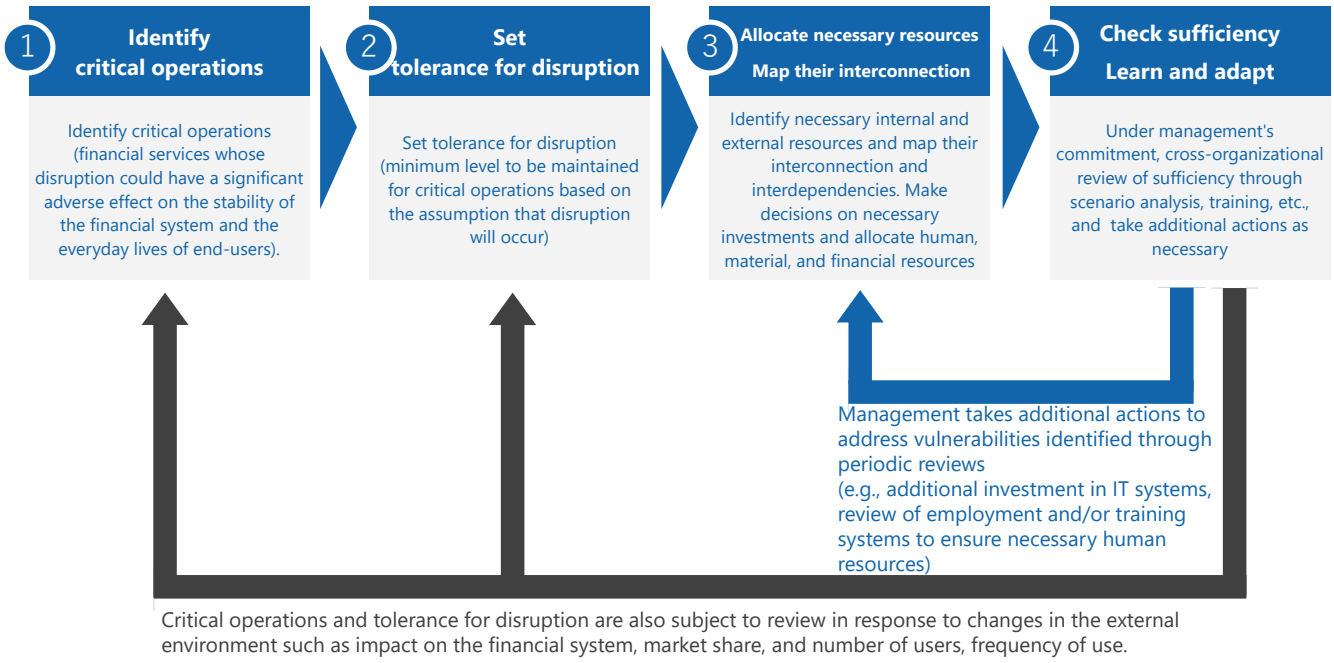
Under these circumstances, existing risk management strategies and business continuity plans (BCPs) may not be sufficient to maintain critical operations for the financial system (e.g. settlement services) when an unexpected event occurs. Thus, it is crucial to develop a framework that will ensure early recovery and mitigation of its impact through alternative means from the user's perspective, assuming that business disruption can inevitably occur even after all preventive measures are taken. It is globally recognized that ensuring operational resilience is material and a comprehensive framework should be developed that covers entire business processes, including outsourced operations and external third-parties' services integrated through APIs.

Taking into account the principles set by the Basel Committee on Banking Supervision in March 2021, this paper defines operational resilience as the ability of financial institutions to continue to deliver critical operations at a minimum level that should be maintained even in the event of system failure, terrorism, cyberattacks, infectious diseases, natural disasters, or other similar events. As shown in Figure 1, the management of financial institutions needs to identify critical operations and, after mapping the interconnection of internal and external business processes, secure the necessary management resources (i.e. human, material, and financial resources) that will keep the impact on the financial system and its users within the tolerance for disruption even in the event of a business disruption or crisis. It also needs to check the sufficiency of such resources through training and testing, and regularly reviewing them during normal operations.

To be effective, it is essential to have an organization-wide understanding of operational resilience as well as top-down commitment by management. It should be noted that many issues are still at the stage of exploring best practices; uniform

standards will not be imposed; a proportionate approach will be taken to reflect the size of the financial institutions, their risk appetite, and their impact on the financial system. Accordingly, this paper aims to present a basic framework for ensuring operational resilience and to summarize issues and challenges to be considered. (See Figure 2)

Figure 1: Basic process to ensure operational resilience



(Source) Financial Services Agency

Figure 2: Challenges and expected benefits of ensuring operational resilience

	Examples of challenges →	Expected benefits
User-oriented financial services	Focus is narrowly placed on preventive measures, resulting in insufficient responses when business disruption actually occurs in times of crisis.	**Minimize impact at times of crisis** from the perspective of users; limit the impact by early recovery, securing alternative means, and prompt publicity.
Efficient overall business processes	Zero tolerance leads to an endless addition of manuals and checklists for preventive measures, which worsens operational efficiencies and exhausts the front-line employees. The business process as a whole becomes inefficient due to silo organization under too many risk and crisis management frameworks.	Based on the recognition that human errors and unexpected events cannot be reduced to zero, formulate realistic tolerance for disruption (minimum levels that should be maintained for critical operations) and **restructure a holistic risk and crisis management framework**; streamline overall business processes with a sense of urgency by utilizing the existing frameworks.
Effective resource allocation	Management resources (human, material, and financial resources) essential to implement the business continuity plan (BCP) are not actually in place. Mapping of the interconnection of internal and external management resources, including third-party vendors, is not sufficient and therefore vulnerabilities have not been identified.	**Identify internal and external management resources essential** to deliver critical operations at the minimum level (tolerance for disruption), and **actually employ, train, and allocate them**, including reviewing governance and personnel system.
Commitment by management	Verification of the appropriateness of the framework has become a mere formality, and adaptation to environmental changes is delayed. The PDCA (plan-do-check-act) cycle is not functioning properly.	**Management should be accountable to stakeholders**, including supervisory authorities, to ensure that they actually allocate necessary management resources.
Corporate culture	Zero tolerance and excessive demerit points system leads to situations where front-line employees may feel intimidated and hesitant to report concerns, and poor coordination between departments.	**Establish strong risk management culture** (e.g., thorough adherence to "Bad News First", free and open dialogue, and cooperation that transcends organizational boundaries).

(Source) Financial Services Agency

2. FSA's Discussion Paper

JFSA's Supervisory Approaches - Replacing Checklists with Engagement (released in June 2018) outlines the basic concepts and approaches common to overall inspections and supervisions of the Financial Services Agency of Japan ("FSA"). Supervisory concepts and approaches for each specific theme and area are shown in the form of theme/area-specific documents ("Discussion Papers"), which serve as references in dialogue between the FSA and financial institutions. This paper is a discussion paper and intended to summarize the issues and challenges for financial institutions in ensuring operational resilience.

Although this paper is primarily intended for banks, it is also designed to serve for discussion with other financial institutions, as it is also important for other companies engaging in critical operations in the financial system to ensure operational resilience.

This paper illustrates the current FSA's views and approaches. As practices and methodologies as well as international discussions to ensure operational resilience are still evolving, it may be revised in the future to reflect progress in those areas. Examples shown in this paper should not be regarded as best practices. They are reference cases as of April 2023.

When the FSA engages in dialogue with financial institutions using this paper as a basis for discussion, it will fully account for the fact that practical approaches to ensure operational resilience and necessary management resources (human, material, and financial resources) may vary among financial institutions depending on the size and characteristics of the services provided by the financial institutions, such as the significance of the financial system, market share, and impact on users. In other words, the FSA will not require financial institutions whose significance in the financial system is relatively small to engage in unnecessarily complex discussions. The FSA does not intend to mechanically and uniformly apply viewpoints raised in this document or use them as a checklist in supervision and inspection.

On 16 December 2022, the FSA published the draft version of this Discussion Paper, and a wide range of public comments were submitted by 16 February 2023. The summary of these comments and the FSA's responses are available on the FSA's website[1]. Taking into account of developments in international discussions and practices, the FSA is committed to hold discussions with stakeholders, including financial institutions and their users, and continuously improve the FSA's discussion with financial institutions.

[1] Financial Services Agency (FSA) (2023) "Results of Public Comments on the Proposed Discussion Paper on Ensuring Operational Resilience" (Japanese)

II. Discussion and background on operational resilience

1. Trends in International Discussions

(1) International principles set by the BCBS

The Basel Committee on Banking Supervision (BCBS) finalized the *Principles for Operational Resilience* (POR)[2] and the *Revisions to the Principles for Sound Management of Operational Risk* (PSMOR)[3] on 31 March 2021.

Both international principles are principles-based and, like other Basel frameworks, are applied on a consolidated basis. While the consistency with the Recovery and Resolutions Plans (RRPs) will be applied to the Global Systemically Important Financial Institutions (G-SIFIs), the other contents of the principles will be applied to financial institutions other than G-SIFIs under proportionality.

The POR consists of seven principles: Governance, Operational risk management, Business continuity planning and testing, Mapping interconnection and interdependencies, Third-party dependency management, Incident management, and ICT including cybersecurity. The details of Principle 2 (Operational risk management) are provided by the PSMOR and both principles should be perceived as practically an integral set of principles to ensure the effectiveness of operational risk management.

In addition, the Financial Stability Board (FSB) published a discussion paper[4] on third-party dependencies and the management of outsourcing contractors as a consultative document to summarize the challenges faced by financial institutions in managing third-party risks in general[5]. The main challenges include: the complexity and lack of transparency in financial institutions' third-party relationships (or supply chain of technologies and services provided); treatment of intra-group outsourcing; concentration risk: substitutability; fragmented supervisory and

[2] Basel Committee on Banking Supervision (BCBS) (2021a) "Principles for operational resilience"
[3] BCBS (2021b) "Revisions to the principles for the sound management of operational risk"
[4] Financial Stability Board (FSB) (2020) "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper"
[5] FSB (2021) "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Overview of Responses to the Public Consultation"

industry practices; data localization requirements; cyber and data security; and constraints in the relevant resources and skills. Under these circumstances, The *FSB Work Programme for 2022*[6] also identified enhancement of operational resilience as one of the priority areas. Specifically, discussions are underway regarding supervisors' expectations on third-party risk management by financial institutions and the harmonization of terminology and definitions.

The International Organization of Securities Commissions (IOSCO)[7] has been discussing management of outsourcing and lessons learned from the COVID-19 pandemic. The International Association of Insurance Supervisors (IAIS) has also published an issues paper on operational resilience as a consultative document[8].

(2) Developments by major overseas supervisory authorities

Alongside the BCBS's finalization of the POR/PSMOR, supervisory authorities in the UK, Europe, and the US have issued regulations and guidance on operational resilience. Although minor differences exist in the terminology used by each supervisor, the concepts align with the international principles of the BCBS, and there is a common understanding that fragmentation of regulation and supervision of internationally active financial institutions should be avoided. Below is an overview of developments in each jurisdiction.

In the UK, the authorities jointly published a discussion paper[9] in July 2018, and then finalized new regulations[10] in March 2021 after public consultations (at the same time, new regulations focusing on third-party risk management were also published[11]). These regulations will be applied incrementally: by the end of March 2022, financial institutions are required to identify their important business services, map management resources that support the important business services, set

---

[6] FSB (2022) "FSB Work Programme for 2022"

[7] International Organization of Securities Commissions (IOSCO) (2021) "Principles on Outsourcing"
IOSCO (2022) "Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic & lessons for future disruptions"

[8] International Association of Insurance Supervisors (IAIS) (2022) "Issues Paper on Insurance Sector Operational Resilience"

[9] Bank of England (BOE), Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA) (2018) "Building the UK financial sector's operational resilience"

[10] BOE, PRA, and FCA (2021) "Operational resilience: Impact tolerances for important business services"

[11] BOE and PRA (2021a) "Outsourcing and third party risk management"

impact tolerances, and test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios; by the end of March 2025, they must conduct lessons learned exercises to identify, prioritize and invest in their ability to respond and recover from disruptions as effectively as possible.

In the case of a third-country branch (e.g., London branches of Japanese banks), the UK authorities will consider whether the home state's operational resilience regime (e.g., Comprehensive Guidelines for Supervision) is sufficiently robust to deliver outcomes similar to those required by the UK regime, including whether the home state supervisor has adopted the POR and whether the firm can demonstrate that it is in compliance with its home state regime[12]. In addition, a proposal to amend the law to give supervisors the authority to directly oversee critical third-parties is under consideration, and a related discussion paper[13] was jointly published by the UK authorities in July 2022.

In Europe, the European Commission published a draft regulation on operational resilience, Digital Operational Resilience Act (DORA)[14], in September 2020. The European Council and the European Parliament reached a provisional agreement on the DORA[15] in May 2022, after public consultations. Similar to the proposed law in the UK, the DORA allows supervisory authorities to directly oversee critical ICT service providers (third-parties).

In the US, the authorities jointly issued guidance[16] in October 2020. This does not impose new regulations but is a comprehensive compilation of existing regulations, guidance, and industry standards applicable to banks above a certain size.

[12] BOE and PRA (2021b) "International banks: The PRA's approach to branch and subsidiary supervision"
[13] BOE, PRA, and FCA (2022) "Operational resilience: Critical third parties to the UK financial sector"
[14] European Commission (EC) (2020) "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014"
[15] Council of the European Union (2022) "Digital finance: Provisional agreement reached on DORA"
[16] Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Federal Reserve Board (FRB) (2020) "Sound Practices to Strengthen Operational Resilience"

2. Changes in the domestic and international environment

As the use of technology in financial services increases, it brings various benefits like improved user convenience, cost savings, operational efficiency, and innovation. However, it also increases dependence on IT systems in the business operations of financial institutions.

Recent years have seen a shift in the approach to IT system development due to an uncertain business environment. Traditionally, large-scale system development has been conducted in an on-premise environment using a waterfall development method[17] and outsourcing to external IT vendors. However, such an approach often led to over-investment or under-investment in response to fluctuations in actual transaction volume, and there was difficulty in responding quickly to changes in transaction volume. As a result, there is now a move towards a more user-oriented approach optimizing investments and quickly adapting to changing transaction volumes by utilizing cloud environments and agile development methods.

This restructuring of business processes to optimize user value can also imply changes in internal management methods, personnel systems, reorganization of in-house and outsourced processes, and collaboration with FinTech companies and other service providers. Therefore, the interconnection of internal and external management resources may be further complicated by digitalization.

The interdependence between internal personnel, facilities, and IT systems, as well as external third-parties (e.g., outsourcing partners, service collaboration partners, service providers, and procurement partners), and fourth-parties (e.g., subcontractors)), has increased. Identifying vulnerabilities throughout the entire business process and understanding and managing the impact of failures or defects in one area to other areas has become a critical international issue. Consequently, third-party and fourth-party risk management are increasingly important given this complex interdependence.

Furthermore, innovations utilizing distributed ledger technology (DLT) are in progress.

[17] In waterfall development, the development process is sequential. Each step such as definition of requirements and specification, external design, internal design, development, system implementation, testing, and operation, is dependent on the output of the previous step. On the other hand, in agile development, the development process is repeated for each small function, and the function is released quickly to receive users' feedback frequently, aiming to flexibly reflect users' needs.

For example, some financial institutions and Financial Market Infrastructures (FMIs) aim to make more efficient and secure securities settlement infrastructure (T+0 settlement) through primary and secondary market platforms for securities tokens (digital securities) and stablecoins, and standardization of post-trade processing. In addition to such digitalization and streamlining of traditional assets, financial institutions are considering new businesses related to cryptoassets, decentralized finance (DeFi), and non-fungible tokens (NFT), such as custody and marketplaces, which results in increasingly diverse risk profiles.

Regarding the COVID-19 pandemic, financial institutions' Business Continuity Plans (BCPs) have been successful and no significant disruptions to financial services have occurred. This is because they have already assumed the pandemic of new influenza as a risk scenario and the BCP has been useful to the case of new infectious disease. However, increased remote work and external connectivity (and also connectivity by group companies and third-parties) have amplified the risk of external intrusions. Additionally, continued vigilance is needed due to growing cybersecurity threats and geopolitical risks, such as Russia's invasion of Ukraine.

Further to infectious diseases, Japan has also faced repeated natural disasters, such as the Great East Japan Earthquake and numerous floods. It is anticipated that Japan will face further damage from a Nankai Trough Earthquake, a potential earthquake directly under the Tokyo metropolitan area, and increasingly severe flooding in the future. Ensuring redundancy to continue critical operations for the financial system, even during such crises, has been a pressing issue. Consequently, some infrastructure companies with main data centers in the Tokyo metropolitan area are moving their backup centers to the Kansai area.

III. Expected roles of financial institutions

As discussed above, in an era of rapid environmental change and high uncertainty, conventional risk management (framework to prevent accidents and failures before they occur) and BCP (a contingency plan for specific risk events, such as earthquakes) may not be sufficient to deliver critical operations for financial systems in unexpected events.

Therefore, based on the assumption that business disruption is inevitable even after all preventive measures have been taken, it is necessary to develop a framework to keep the impact within a tolerance for disruption from the perspective of users. In other words, rather than just building upon the conventional approach of assuming specific risk events in advance and making a contingency plan (BCP), it is necessary to take a more proactive and reverse stress testing approach (i.e., to assume a certain level of business disruption has occurred, reverse engineer the cause of the disruption and verify where the vulnerability lies and which level of tolerance has been secured). Such approaches are required to adapt to changes in the risk environment and respond to unexpected events.

Specifically, a holistic framework must be established from a new perspective while utilizing existing frameworks divided among various departments such as operational risk management, BCP, RRP, IT system risk management, IT governance, cybersecurity, third-party risk management, conduct risk management, etc. From this new perspective, financial institutions are needed to verify whether the internal and external management resources have actually been secured, that are essential for mitigating the impact and quickly restoring their critical operations when a business disruption occurs. Such a holistic framework with a PDCA (plan-do-check-act) cycle is needed to ensure operational resilience.

In particular, in a silo organization, the development of individual frameworks can lead to excessive or insufficient allocation of management resources. By adopting the new perspective of operational resilience, it is expected that sufficient human, material, and financial resources can be allocated to necessary processes, and excessive processes can be rationalized or eliminated.

The following is a summary of the basic process of operational resilience:

(1) Identify the "critical operations"
(2) Set the "tolerance for disruption" (minimum level of the critical operations to be maintained to mitigate the impact on the financial system and users within a certain range in case of a business disruption)
(3) Map the interconnection of business processes internal and external of the firm, and secure necessary management resources (human, material, and financial resources)
(4) Check sufficiency through periodic reviews such as training and testing, and learn and adapt, taking additional actions to address identified vulnerabilities.

BOX 1: Operational risk management

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Operational risk management encompasses identifying risks to the financial institutions especially in the core products, business processes and systems; measuring, assessing, and monitoring exposures to those risks; taking steps to control or mitigate exposures.

Management's proactive involvement in establishing an operational risk management framework, including personnel management of officers and employees, and periodic reviews on the sufficiency of the framework are also important factors in ensuring operational resilience. In order to establish an operational risk management framework, a policy on operational risk management, a reporting and monitoring system, design of incentives for officers and employees, and an education and training system for risk management, as well as of ethics should be established. Check-and-balance function should be sufficiently exercised based on a three-line defense system consisting of the operations execution department (first line), risk management department (second line), and internal audit department (third line). It is also needed to clearly define procedures on operational flow and operational risk management framework.

Under the Basel III capital framework (Pillar 1), operational risk is one of the major risk categories along with credit risk and market risk[18]. The operational risk capital requirements are calculated by multiplying the Business Indicator Component (which is calculated by interest income and services income) and the Internal Loss Multiplier (which is a scaling factor that is based on a financial institution's average historical losses over the previous 10 years). In addition to accurately and comprehensively capturing operational risk and maintaining financial soundness sufficient to absorb losses when risks materialize through capital requirement, financial institutions must also mitigate operational risk by analyzing the causes of losses and developing measures to prevent recurrence.

It should be noted, however, operational risk management framework alone may not be sufficient when unexpected events occur due to changes in the external environment for which preventive measures have not been formulated in the past. Regarding the quantification of operational risk based on the internal losses over the past 10 years in a backward-looking manner, it should be noted that there is an assumption that events similar

[18] As of end of March 2022, operational risk assets in the banking sector in Japan were approximately 25 trillion yen (approximately 5% of total risk assets).

to those in the past could occur in the future with similar frequency. In this regard, there is a growing international discussions that backward-looking risk measurement may not be sufficient for risks associated with new technologies and environmental changes, such as cyberattacks, artificial intelligence (AI) and machine learning (ML), cryptoassets, or climate change, and that forward-looking risk measurement may be necessary.

In general, in areas where change is rapid and best practices have not yet been established, a uniform standard by regulation may not be feasible, and even excessive regulation may stifle innovation. A flexible supervision is more desirable. The perspective of operational resilience complements the existing operational risk management framework so that supervisors can encourage financial institutions to upgrade their operational risk management through monitoring.

BOX 2: IT systems risk management and cybersecurity

In this era of increasing digitalization and reliance on IT systems, managing risks associated with these systems and maintaining cybersecurity are crucial aspects of operational risk management. The FSA has recognized this and has provided guidance in the form of discussion papers and detailed reports[19].

One aspect that's highlighted is the concept of "cyber hygiene", a reference to the routine practices that help maintain system health and improve online security. Much like personal hygiene practices (like washing hands) help prevent disease, cyber hygiene practices (such as proper IT asset management and promptly applying security patches) can help prevent security breaches. The idea is to cultivate a culture within the organization that fosters these practices and thus enhances security.

As threats evolve and become more sophisticated, it is important not just to focus on preventing cyberattacks, but also mitigate the impacts when incidents do occur. This concept of "cyber resilience" is becoming increasingly vital.

Operational resilience, however, extends beyond IT risk management and cybersecurity. It's

[19] FSA (2019) "Discussion Paper on Dialogues and Practices Regarding Financial Institutions' IT Governance"
FSA (2022a) "Survey Report on Financial Institutions' IT Governance and Related Matters" (Japanese)
FSA (2022b) "Analysis Report on System Failures in Financial Institutions" (Japanese)
FSA (2022c) "Policy for Strengthening Cybersecurity in the Financial Sector (Ver. 3.0)" (Japanese)

about being able to respond flexibly to crises, allocating resources effectively under normal conditions so that the institution is prepared for adverse situations. In a practical sense, this means, for example, if there is a failure in the institution's ATM systems, not only is it crucial to restore the system as quickly as possible, but also important to keep users informed and provide them with alternatives (like using other ATMs or online banking). This approach, which prioritizes minimizing disruption for users, is a key element of ensuring operational resilience.

1. Identify "critical operations"

Financial institutions should identify their "critical operations." Critical operations are those financial services whose disruption could pose a significant adverse effect on the stability of the financial system or on the everyday lives of end-users.

To pinpoint these critical operations, financial institutions may utilize existing Business Continuity Plan (BCP) and Recovery and Resolutions Plan (RRP) frameworks from the perspective of users. Specifically, factors that should be taken into account are: potential impact of disruption of critical operations on the maintenance of the functions of the financial system, the size of the financial institution, its market share, the number of users, the frequency of service use, the institution's revenue and market credibility, and the possibility of service substitution by other institutions.

For instance, under existing BCP frameworks[20], certain financial services are considered crucial for maintaining the functions of the financial system. These include the processing of large-lot, large-volume settlements conducted through the interbank market and the interbank settlement system, acceptance of individual users' requests for cash withdrawal and remittance, and bill clearing. Such services could potentially be defined as critical operations in the context of operational resilience.

Existing BCP frameworks at financial institutions[21] often select services with a high market share, such as funds settlement and lending, as targets for continuity during crises due to their significant impact on the financial system and their users. Thus, these existing frameworks could be useful when determining critical operations for the sake of operational resilience.

[20] FSA (2023) "Comprehensive Guidelines for Supervision of Major Banks, etc"

[21] Bank of Japan, Financial System and Bank Examination Department (2015) "Questionnaire Survey on Business Continuity Management (September 2014)"

BOX 3: Business Continuity Plan and Recovery and Resolutions Plan

(Business Continuity Plan)

In order to take swift recovery measures and ensure that the minimum necessary operations and services are maintained in the event of an emergency, financial institutions need to make appropriate preparations in normal times. This includes establishing Business Continuity Management (BCM) systems and formulating Crisis Management (CM) manuals and a Business Continuity Plan (BCP).

BCP is a crucial component of operational resilience. In practice, many financial institutions consider how to ensure operational resilience based on the BCP frameworks. It is important to note, however, that the BCP often involves formulating individual crisis management manuals based on the assumption of specific types of crises, such as:

(1) Natural disasters (earthquakes, wind or flood damages, abnormal weather, epidemics of infectious diseases, etc.)
(2) Acts of terrorism and wars (including those that occur outside Japan)
(3) Accidents (large-scale power failures, IT system failure, etc.)
(4) Unfounded/harmful rumors (word-of mouth rumors, Internet messages, e-mail messages, news articles based on speculation, etc.)
(5) Crimes committed against banks (cyberattacks, blackmail, intervention by anti-social forces, data theft, and abduction of officers or employees)
(6) Problems involved in business processes (responses to complaints and inquiries, errors in data entry, etc.)
(7) Problems related to personnel management affairs (accidents and crimes involving officers and employees, internal disputes, sexual harassment cases, etc.)
(8) Problems related to labor affairs (cases of whistle-blowing, deaths from excessive workloads, occupational diseases, drain of human resources, etc.)

In a rapidly changing risk environment, the BCP alone might not be sufficient to respond to severe but plausible unexpected events. For this reason, a comprehensive operational resilience framework is required to verify the functionality of the existing framework, including the BCP, in a cross-organizational and comprehensive manner, and to enhance the framework as necessary.

Additionally, to ensure the effectiveness of the BCP, including crisis management manuals, it is necessary to identify, invest, and allocate the internal and external management resources (human, material, and financial resources) essential to mitigate the impact of the

business disruption, and to take initial actions for quick recovery. Operational resilience isn't just about formulating a BCP; it also involves checking the sufficiency of the plan. If the allocation of management resources is found to be insufficient, the management must make decisions on additional investment[22].

There is a shift from the conventional (disaster-based) BCP, which is formulated for each type of crisis (cause of business disruption), to the all-hazard (consequence-based) BCP. The latter doesn't assume a specific crisis but instead assumes business disruption and ensures initial response and recovery procedures, as well as alternative means. Practical efforts for such all-hazard BCPs are overlapping with those for ensuring operational resilience.

(Recovery and Resolutions Plan)

Based on reflections on the Global Financial Crisis, Global Systemically Important Financial Institutions (G-SIFIs) and financial institutions deemed by the home authority to have a potential impact on financial stability in the event of their bankruptcy are globally required to develop robust and credible Recovery and Resolutions Plans (RRPs).

The purpose of RRPs is to end the so-called "too big to fail" problem, which refers to the issue whereby national authorities are not able to resolve globally active banks and have no option but to rescue them by injecting public funds due to the concern that unorderly failure of such financial institutions would have an extremely serious adverse effect (the "systemic risk") on financial and economic systems in each country. In normal times, financial institutions are required to develop their recovery plans and organizational arrangement that prevent crisis situations to develop into the failure of the institutions, and increase their resolvability should they fail. Resolvability of a financial institution means the state in which it is feasible and credible for the resolution authorities to resolve it in a way that protects systemically important functions without causing severe systemic disruption and without exposing taxpayers to loss.

[22] Business Impact Analysis (BIA) can also contribute to ensuring the BCP and therefore operational resilience. Generally, in a BIA, a firm identifies critical operations that should be prioritized for recovery in the event of a disaster, sets a Maximum Tolerable Period of Disruption (MTPD) and a shorter Recovery Time Objective (RTO), and identifies necessary management resources, based on the impact on stakeholders when such operations are disrupted. It is also possible to set a Recovery Level Objective (RLO) to determine the level of recovery in the RTO, and a Recovery Point Objective (PRO) to determine the point in the past when the data is to be recovered. The minimum level of operations and services to be delivered even after a crisis is defined as the RLO in the short term, but it can be defined as a Minimum Business Continuity Objective (MBCO) in the longer term.

Financial institutions are required to identify critical functions, the failure of which would lead to a severe disruption of the financial system[23]. To ensure operational resilience, a similar process is also required from the user's perspective. Some financial institutions are considering identifying their critical operations, utilizing the critical functions of the RRP, in addition to utilizing the BCP.

2. Set "tolerance for disruption"

Financial institutions should establish their risk appetite[24] and tolerance for disruption for identified critical operations, i.e., a minimum service level to be maintained based on the assumption that business disruption will inevitably occur even after all preventive measures are taken.

The tolerance for disruption typically aligns with the Recovery Time Objective (RTO) set in the BCP. However, from the perspective of mitigating the impact on the financial system and users' everyday lives within a certain range, financial institutions can also consider other factors such as scope of business disruption, the number or amount of transactions, and the number of users affected (e.g., the number of complaints from users at the time of business disruption).

According to the minimum RTO set in the existing BCP framework[25], operations "especially vital for the maintenance of the functions of the financial system, such as the processing of large-lot, large-volume settlements conducted through the interbank market and the interbank settlement system" are required to "recover within the same day when a business disruption occurs."

In practice, many financial institutions set an RTO of "within 4 hours" to "within the same day" for funds settlements and cash withdrawal and remittance, which should be restored with the highest priority in a crisis[26]. It would be beneficial to utilize such existing frameworks when considering tolerance for disruption in terms of operational resilience.

---

[23] FSB (2013) "Guidance on Identification of Critical Functions and Critical Shared Services"

[24] Risk appetite is defined as the aggregate level and types of risk a financial institution is willing to assume to achieve its strategic objectives or business plan within its risk capacity (the maximum level of risk the financial institution can assume).

[25] FSA (2023) "Comprehensive Guidelines for Supervision of Major Banks, etc"

[26] Bank of Japan, Financial System and Bank Examination Department (2015) "Questionnaire Survey on Business Continuity Management (September 2014)"

Mitigating the impact on the financial system and the lives of users does not necessarily mean focusing solely on the recovery of one's own IT systems. While early restoration of the IT system itself is still important, from the user's perspective, timely communication about the failure and publicity about alternative access means are also important.

It should be noted, however, that if many financial institutions depend on a specific alternative, then a wide-area disaster could disrupt their business operations, including the alternative (See [BOX 9: Third-party risk management (4): Strengthening cross-industry initiatives] for more information on managing the concentration risk on a specific third-party across the industry).

BOX 4: Service Level Objective and Tolerance for disruption

More financial institutions are adopting public cloud services to flexibly respond to changes in transaction volume. This is especially beneficial in an uncertain business environment where it's difficult to predict users' service demands. In delivering financial services within such a cloud environment, setting a high Service Level Objective (SLO) faces a trade-off with increased costs. Therefore, some financial institutions aim to strike a favorable balance between cost and convenience from the user's perspective. To do this, they publish their SLOs (defined in terms of availability and downtime) and operation results for each financial service, depending on its importance.

For instance, if improving availability from 99.99% to 99.999% increases costs by a factor of 10, will users truly value this high availability enough to justify the cost? Or would they prefer lower costs if they can tolerate occasional downtime? Perhaps they might value other conveniences, such as ease of access? These questions cannot be definitively answered in advance and will ultimately be determined through market competition as financial institutions offer a variety of services.

While an SLO differs from the concept of tolerance for disruption, they are closely related from the user's perspective.

3. Map interconnection and secure necessary management resources

Financial institutions should identify the internal and external management resources (human, material, and financial resources) throughout the entire end-to-end business process essential for delivering critical operations at a tolerance for disruption. After mapping their interconnection and interdependence, they need to employ and assign officers and employees with necessary skills and expertise, procure and secure appropriate facilities, IT systems, third-party services, etc., and make sufficient investments for their maintenance and improvement.

Considering that the increasing complexity of interconnection between financial institutions and third-parties, it may be useful for them to regularly report and share information with the supervisory authorities regarding their use of critical third-party services. This will allow the authorities to grasp the concentration risk of specific third-parties and to engage in dialogue with such critical third-parties. Such a step may contribute to the resilience of the financial system as a whole.

BOX 5: Scope and granularity of mapping of interconnection

One issue is determining the scope and granularity of the mapping of interconnection and interdependence of internal and external management resources essential for financial institutions to deliver their critical operations at a minimum level (tolerance for disruption).

For instance, a bank's IT system consists of various interdependent modules, including the core banking system, information system, external connection system, and other internal contact systems. If the management team, including the CIO or CTO, doesn't understand these systems' configurations, it becomes difficult to predict potential system failures. Understanding the interdependence among these modules within its own IT systems is crucial when setting the tolerance for disruption of critical operations. It is clearly important to fully verify such interdependencies in the system development testing process to prevent system failures. However, in the current severe profit environment, there are instances where costs and schedules are inevitably prioritized, resulting in financial institutions being unable to ensure operational resilience.

Besides the IT system aspect, it is also necessary to map the interconnection in terms of operations. Financial institutions must document how many people, with which skills and

capabilities, are needed at which facilities and in which departments during normal times (how many are exclusively in charge, how many are concurrently in charge, and how many are BCP personnel when switching to manual operations). They need to outline the decision-making process for switching to a backup data center if the main data center fails during a crisis, and identify what kind of management resources are needed in the end-to-end business process. It's necessary to understand how a lack of management resources in one part of the business process (e.g., personnel shortage due to disaster, damage to facilities, hardware failure, etc.) will spill over to other parts of the business process. In this case, a reverse stress testing approach may also be beneficial.

The practical challenge of mapping interconnection is with regard to external management resources. Financial institutions depend on external third-parties (e.g., outsourcers, external service providers integrated through API, public cloud service providers, procurement partners) and fourth-parties (e.g., subcontractors). In international discussions, critical third-parties often include IT vendors outsourced for system development and operation, and public cloud service providers. Additionally, API integration with external services provided by FinTech firms is also increasing. For example, a system failure of an external partner whose service is SMS identity authentication can cause financial service disruptions for mobile app users. Disruption of communication and electricity also significantly impacts the delivery of financial services, and therefore financial institutions are supposed to secure redundant communication lines and private power generators. Financial market infrastructures (e.g., BOJ-NET, Zengin system (Japanese Banks' Payment Clearing Network)) and security companies that handle cash transportation can also be critical service providers. It's also important to understand the interconnection with Nth-parties (subcontractors, sub-subcontractors, and so on).

There can be a variety of practices regarding mapping of interconnection. A basic method is to create a business process flowchart and list the related management resources. Another method is to visualize the geographical concentration of management resources, such as a main data center, backup center, and third-party IT system locations to estimate the geographical impact of risks such as earthquakes, floods, infectious diseases, terrorism, and wars.

It is worth noting that such interconnection mapping is intended to help financial institutions identify the management resources (human, material, and financial resources) essential to ensure operational resilience. Therefore, the scope and granularity of the mapping would be to the extent necessary for this purpose.

BOX 6: Third-party risk management (1): Strengthening monitoring by individual financial institutions

By mapping the interconnection of internal and external management resources, financial institutions are supposed to identify critical third-parties that are essential to delivering their critical operations at a minimum level (tolerance for disruption). They should then conduct third-party dependency management, or third-party risk management, such as confirming and maintaining the quality of the third-party services, securing alternative means, and developing exit strategies[27].

In particular, approaches to mitigate the risk of concentration in specific third-parties can be categorized into four types: (1) strengthening the monitoring of third-parties by individual financial institutions, (2) securing alternative means and exit strategies, (3) insourcing, and (4) strengthening cross-industry initiatives.

Currently, financial institutions are conducting a certain level of monitoring of third-parties, such as IT vendors. This includes requiring them to: disclose information prior to entering into contracts; disclose timely and detailed information in the event of business interruption; ensure business continuity and data security; and conduct periodically joint training and testing. In particular, confirmation of contractual relationships with fourth-parties (whether the third-party uses subcontractors or cloud services) is important to mitigate risks such as unauthorized actions or leak of information by the Nth-parties. In addition, some financial institutions are checking reputation of the Nth-parties and developing other measures to mitigate potential risks.

However, major financial institutions may have thousands of third-parties, and even if they focus on critical ones, the number of third-parties may range from a few dozen to several hundred. It is practically challenging to require uniform standards for all of them. Therefore, monitoring needs to be conducted in a manner that is appropriate to the level of materiality and risk assessment.

In terms of obtaining appropriate information before concluding a contract, it is important to conclude a Service Level Agreement (SLA) that clearly states the third-party's guarantee

[27] BCBS (2021a) "Principles for operational resilience" defines "third-party dependency management (Principle 5)" as the management of third-party risk, which is the risk in the event of a failure or disruption at the third-party impacting the provision of critical operations. Financial institutions should verify whether the third-party at least equivalent level of operational resilience to safeguard the financial institutions' critical operations in both normal circumstances and in the event of disruption.

of service level (definition, scope, content, quality, downtime, etc.) and to ensure consistency with the tolerance for disruption. For example, if the availability on the SLA of a cloud service provider is 99.99%, the availability of financial services that run on such an infrastructure is supposed to be less than that. It is necessary to balance availability and cost in light of what users want.

To monitor the level of third-party service after the contract is concluded, in addition to desk training and written checklists and monitoring of financial information, joint BCP training based on common test scenarios such as ransomware damage and periodic on-site inspections may be considered.

However, the FSA has heard that it is sometimes more difficult to get major cloud service providers to disclose timely and detailed information in case of business disruption for contractual or security reasons, compared to conventional outsourced IT vendors. In such cases, regardless of individual financial institutions' efforts to strengthen monitoring, there are certain limits to the level and extent of their controls.

In international discussions, major cloud service providers are often regarded as critical third-parties due to their degree of oligopoly in the market and the significant impact they have on critical operations when adopted as the infrastructure for a core banking system of a financial institution. The risk of concentrated use of a single cloud services provider is one of the issues that should be noted, as the failure of such a provider could potentially spill over into systemic risk.

The essential issue in the approach of strengthening monitoring by individual financial institutions is that outsourced operations are outsourced because the financial institution's own management resources are insufficient or deemed inefficient in the first place. Therefore, the incentive to continue to have the human resources to understand the outsourced operations, detect problems, and respond to them is often lacking. Given such an incentive structure, even if on-site inspections are formally conducted, monitoring may become a mere formality due to the lack of know-how among in-house personnel in the first place.

One example of a practical approach to improving the efficiency and effectiveness of monitoring is to conduct joint audits of IT vendors by regional banks that operate joint system infrastructures for those banks. Another good example of efficient and effective monitoring is a case in which a third party organization consisting of bank alumni, researchers, and security consultants checks on a daily basis (e.g., checking procedures and providing advice on BCP training scenarios). To eliminate the inefficiency of individual

financial institutions conducting their own audits, external audits can be used for collective monitoring, such as the use of SOC (Service Organization Control) reports[28] for internal controls of outsourced service, including cloud services. In the case of SaaS, the registration status with the "Information system Security Management and Assessment Program (ISMAP)"[29] is also used as reference information.

Other voluntary efforts by the industry are also progressing. For example, the Center for Financial Industry Information Systems (FISC) has developed and revised the "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions" and the "Manual for the Development of Contingency Plans in Financial Institutions (Plans for Measures in the Event of Emergencies)."

BOX 7: Third-party risk management (2): Securing alternative means and exit strategies

One approach that financial institutions can take to reduce their dependence on specific third-parties is to secure alternative measures and exit strategies. Financial institutions have already decided what kind of redundant configuration they will adopt for each business that is placed on the cloud in preparation for system failures and natural disasters.

Some banks that have built their core banking systems on public cloud services have adopted not only multi-zone backups in the event of local failures, but also multi-region backups (specifically Tokyo region and Osaka region) to deal with large-scale failures or wide-area disasters. Considering a trade-off between the degree of availability required, cost, and service speed (the higher the redundancy, the lower the speed), financial institutions must find a balance.

Another example of redundancy at the cloud services provider level is a multi-cloud environment in which two or more public cloud services are used in combination. However, many stakeholders have said that multi-cloud is currently difficult due to the cost bottleneck

[28] SOC report is a report by an auditing firm or a certified public accountant that describes the results of an objective examination of the effectiveness of internal controls at a trustee company for a specific task, when the task is outsourced and provided by an external party, from the standpoint of an independent third party.

[29] ISMAP is a system operated by the National center of Incident readiness and Strategy for Cybersecurity (NISC), the Digital Agency, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry to ensure the security level of cloud services procured by the government by evaluating and registering cloud services that meet government security requirements in advance and to contribute to the smooth introduction of cloud services.

of training or hiring personnel who can handle the different specifications of each cloud platform.

Another issue is the risk of geographic concentration. In Japan, data centers of major cloud services providers must be located near Tokyo to secure engineers to work in their data centers, but there are only a limited number of specific locations with relatively low disaster risk, resulting in a geographic concentration. Any areas in Japan could be damaged by natural disasters. Such geographic concentration risk (vulnerability to disasters and infectious diseases) also applies to conventional IT vendors that operate joint IT systems for financial institutions.

It should be noted, however, that some stakeholders have said that rather than the risks associated with adopting open systems and public cloud services, one should keep in mind the risk of being left behind by changes in the external environment and having systems continue to deteriorate by not embracing such new technology.

In other words, when financial institutions utilize software to conduct their business, they need to regularly update their systems in response to changes in the external environment, such as technology and human resources, to prevent deterioration in quality. In this regard, open systems using general specifications and publicly available technologies and cloud services operated by major cloud service providers with a high market share have been evaluated as highly versatile and portable, and easily adaptable to changes in the external environment.

BOX 8: Third-party risk management (3): Insourcing

Financial institutions can reduce their dependence on specific third-parties by bringing outsourced operations in-house. Identifying the internal and external management resources needed to deliver their critical operations with a tolerance for disruption requires skilled and experienced personnel. Securing specialized human resources in-house is essential to ensure operational resilience.

Controllability, particularly when making decisions regarding IT system development without solely relying on outsourced IT vendors, is crucial for financial institutions. They should take the initiative in deciding what to create, how to design software, which technology to use, which service structure to adopt, and who should develop (code) these systems. Additionally, they need to assess and control the quality of the code delivered by the IT vendor. Rather than following the IT vendor's instructions blindly, financial institutions should communicate with the vendor on an equal footing to maintain control over their

systems.

Some financial institutions are insourcing IT personnel to ensure controllability. Recognizing that a seniority/membership-based wage system may not attract highly skilled IT personnel, some have established subsidiaries with different personnel management system from that of the headquarters. They are trying to secure the necessary human resources by competing with IT firms in recruitment, offering attractive conditions such as an annual salary system, discretionary labor systems, flexible hours, and full remote working options.

It should be noted that young engineers tasked with maintaining legacy systems often change their firms for opportunity to refine their high-market-value skills. As engineers capable of handling these legacy systems age and retire, there would be no personnel within the company or at vendors who can replace the systems. To avoid such a crisis, it is an urgent task for financial institutions to consider the ease of procuring engineers and establishing a wage structure that attracts top talent. This is not only vital for digital transformation or innovation promotion, but also for ensuring operational resilience.

Outsourcing IT system development and operation to a joint system arrangement of multiple financial institutions also has both advantages and disadvantages. While reliance on the joint arrangement can make it challenging to recruit and train in-house IT personnel, there are strategic benefits in terms of economies of scale and cost savings. Even in terms of BCP effectiveness and IT system stability, the joint implementation can contribute to the establishment of a backup center, which may otherwise be difficult and expensive to set up by a single financial institution. Vendor monitoring can also be conducted more efficiently through joint implementation.

BOX 9: Third-party risk management (4): Strengthening cross-industry initiatives

Possible approaches that individual financial institutions can take to mitigate third-party risk include (1) strengthening monitoring, (2) securing alternative measures and exit strategies, and (3) insourcing. However, these approaches have efficiency challenges. For financial institutions where necessary human resources and expertise have been depleted in-house, effectiveness also poses significant challenges.

Beyond ensuring operational resilience at individual financial institutions (or "micro-operational resilience"), there is a risk that rational actions of individual institutions may undermine the stability of the entire financial system, a fallacy of synthesis. For example, while using services provided by major third-parties can reduce costs and promote digital

transformation for individual financial institutions, systemic risk may arise if these services are disrupted due to system failures or disasters[30].

To maintain a minimum level of critical operations (i.e., tolerance for disruption), it is important to ensure operational resilience across the entire financial ecosystem (or "macro-operational resilience"). This includes IT vendors, FinTech companies, financial market infrastructure, security companies, telecommunications companies, electric power companies, and other critical third-parties.

The FSA monitors financial institutions' outsourcing partners to understand associated risks. In case of system failures, the FSA has the authority under the Banking Act to issue an order to report relevant matters to the third-parties responsible for system development and operation. This allows the FSA to analyze the cause, understand measures to prevent recurrence, and confirm the adequacy of the risk management framework, including that of third-parties. Going a step further, it would be of some significance for the FSA to hold dialogue with critical third-parties, such as major IT vendors, including operators of joint IT systems for financial institutions, from the perspective of understanding the concentration risk.

In line with global trends, many major jurisdictions have adopted a supervisory approach in which supervisory authorities collect reports on third-party usage from financial institutions. This helps identify third-party concentration risk by business type and region. In the UK and Europe, supervisory authorities are considering new regulations to oversee critical third-parties directly. This might be more efficient for society as a whole than individual financial institutions managing their own third-party concentration risk [31]. Also, to avoid fragmentation of regulation and supervision in each jurisdiction for global third-parties such as major cloud services providers, the need for an internationally coordinated oversight by supervisors from major jurisdictions, similar to the coordinated oversight to SWIFT (Society for Worldwide Interbank Financial Telecommunication), has also been discussed[32].

[30] Juan Carlos Crisanto, Johannes Ehrentraud, Marcos Fabian and Amélie Monteil (Financial Stability Institute of the Bank for International Settlements) (2022) "Big tech interdependencies - a key policy blind spot"

[31] BOE and PRA (2021a) "Outsourcing and third party risk management"
EBA (European Banking Authority) (2019) "Guidelines on outsourcing arrangements"
United States Congress (1982) "US Code Tittle 12 Chapter 18 Section 1867 (Bank Service Company Act)"

[32] Jermy Prenio and Fernando Restoy (Financial Stability Institute of the Bank for International Settlements) (2022) "Safeguarding operational resilience: the macroprudential perspective"

However, securing human resources and know-how at supervisory authorities poses practical challenges. In rapidly changing areas where best practices have not yet been established, uniform regulation may stifle innovation. A flexible supervisory approach that explores best practices through dialogue with private-sector stakeholders may be preferable.

It's worth noting that cross-industry training and exercises can help ensure the operational resilience of the entire financial system. For example, the Bank of Japan ("BOJ") regularly conducts market-level BCP drills[33] in the money market, securities market, and foreign exchange market. On the request of money market participants, the BOJ's Financial Markets Department also conducts Funds-Supplying Operations against Pooled Collateral starting on the same day for training purposes, providing an opportunity to verify operation flows in the event of a disaster, such as bidding and funding operations from backup locations, assuming a communication disruption between Tokyo and Osaka. While some of these cross-industry exercises are sponsored by industry associations like the Japanese Bankers Association, the public sector, with its broader perspective, could play a greater role.

BOX 10: Personnel system to secure necessary human resources (Membership-based/Job-based)

To ensure operational resilience, financial institutions must continually improve their IT systems in response to external changes. Realistic tolerance for disruption should be set under the leadership of management, with decisions on additional investments made if management resources are insufficient. The management should be accountable to stakeholders, including supervisory authorities. For instance, CIOs or CTOs should be assigned as specialists who understand their firm's IT systems at a level that allows them to read and write code and understand risks, and employ and train the necessary advanced IT personnel.

However, given the shortage of high-level IT personnel in Japan, securing the necessary human resources is not easy. There have been cases where personnel with no expertise have been assigned as CIOs, and in some cases, cost reductions have been prioritized and insufficient budgets have been allocated for IT system maintenance, resulting in large-scale system failures.

[33] Bank of Japan, Financial Markets Department (2022) "Market-Level BCP Joint Exercises for Three Markets" (Japanese)

While lack of governance is the primary cause of management's failure to secure necessary resources, some experts believe the Japan's unique membership-based personnel system may also be a contributing factor. For example, a membership-based personnel system does not clearly define job descriptions and requirements of skills, abilities, or experience that are needed to perform the job. Instead, the management employ new graduates without defining clear job descriptions and train them on-the-job. In addition, periodic job rotation makes it difficult for employees to develop expertise as their jobs change over the course of several years.

On the other hand, the job-based personnel system common in other jurisdictions clearly defines jobs in the employment contract and job description. Only those capable of performing the job are hired, making this system more compatible with the concept of operational resilience in which management defines the management resources needed to deliver critical operations at tolerance for disruption, and then recruits and assigns personnel who meet the requirements.

Some companies are gradually reviewing the career paths for the employees and wage systems to make it easier to recruit and train engineers, so best practices are still being explored at this juncture.

4. Check sufficiency, learn and adapt

Under the leadership of their management, financial institutions should periodically and cross-organizationally check and review the sufficiency and appropriateness of their risk appetite, critical operations, tolerance for disruption, and essential management resources. This will be achieved through an analysis and exercise based on extreme but plausible scenarios, and additional actions taken as necessary based on lessons learned.

Typically, after a periodic review identifies vulnerabilities, more human, material, and financial resources should be invested. The additional actions might include reassessing the quantity of critical operations and tolerance for disruption in response to changes in the external environment. Other potential measures include reevaluating the corporate culture or personnel system, encompassing employment and training systems.

In this context, "establishing a strong risk management culture" (Principle 1), as stated in the PSMOR, is a crucial element. It ensures a flexible response to crises from the user's perspective, promptly reporting any issues or problems that may impact the users to the top management and relevant departments without neglecting the problem ("Bad News First") and fostering frank dialogue.

However, if the management fails to foster a speak-up culture or if the corporate culture exhibits certain features—like poor inter-departmental coordination, frequent careless mistakes, high turnover, management not providing growth opportunities for subordinates, yearly reorganizations without actual business impact, or major policies decided before thorough discussion—any additional measures taken will be merely perfunctory, far from ensuring operational resilience.

To ensure operational resilience, financial institutions need to foster cross-departmental collaboration—between system development and operation, operations, public relations, and external third-parties—and continue the PDCA (plan-do-check-act) cycle for preparation and allocation of management resources for swift recovery. This includes securing alternative means, from the user's perspective. To facilitate such collaboration, it's crucial to encourage open dialogue among personnel and organizations with different values, expertise, and backgrounds, promoting the understanding and appreciation of diversity.

However, it is noted that financial institutions are still in the stage of exploring best practices among various methods. In a trial-and-error process, it would be understood what types of incentive design, code of ethics, and specific actions are necessary. The examples provided are purely for reference.

BOX 11: Strong risk management culture (1): Just Culture

In practice, some financial institutions borrow from the risk management culture (Just Culture) of other infrastructure industries such as airlines, railroads, and healthcare. A demerit points system that treats human error as the root cause of incidents and imposes penalties (such as pay cuts, suspensions, retraining, and prosecution) on involved individuals can discourage the sharing of potential risks. These may include workplace concerns and discomfort, potentially delaying initial response to a crisis. Instead, human error should be viewed as an indicator of organizational issues, such as insufficient personnel or training, or poor interdepartmental communication or cooperation. Incidents and near-misses should be seen as opportunities for the entire organization to learn and adapt. Based on this human-factors engineering knowledge, some financial institutions have abolished penalties for individuals who made clerical errors and demerit points in personnel evaluations.

While concealment of clerical errors or intentional internal fraud must still be penalized, it is vital to create incentives for frontline staff to promptly and openly report incidents and concerns to their managers and relevant departments. Such incentive designs are crucial to maintain financial soundness by accurately and comprehensively identifying operational risk and estimating capital requirements. (See [Box 1: Operational risk management])

BOX 12: Strong risk management culture (2) (Psychological safety)

Establishing a sound and open corporate culture that promotes prompt information sharing and frank discussion requires the assurance of psychological safety. This means fostering a work environment where individuals can ask questions, voice their concerns, and behave candidly without fear of repercussions.

Factors such as quota supremacy, psychological pressure, and unclear directives can undermine psychological safety, often leading to violations of user protection. A corporate culture that lacks psychological safety can also hinder inter-organizational cooperation.

In a crisis situation where the impact on users and the cause are not well understood, there needs to be a corporate culture and incentive design that rewards proactive and voluntary actions to prevent harm by speaking up across organizational silos and working together from the user's perspective. This is true even if the actions are later found to have been misguided.

However, in organizations where a stringent demerit points system is prevalent, proactive and voluntary attitudes will not be rewarded. Instead, any errors will be severely penalized,

making it risky for frontline staff to voice their concerns. As a result, inaction may seem like the most rational choice. Ensuring psychological safety in the workplace is a critical factor in promoting effective inter-organizational cooperation during crises.

Various concrete methods can help ensure psychological safety and foster a speak-up culture. One such example is the one-on-one meeting, increasingly introduced in both public and private sectors across various industries. This dialogue between manager and team member is not a one-way instruction or lecture but an opportunity to understand the member's concerns and unease. It is expected to nurture the member's independence and spontaneity through questioning and listening that delves into their problem consciousness and discomfort, rather than one-way instructions and preaching.

In addition, communication methods like two-on-two meetings and trialogues are being introduced in the public and private sectors. While one-on-one relationships tend to inevitably result in a not-so-flat exchange of opinions due to the inevitable power gradient between the evaluator and the evaluated, such communication methods based on the reflecting process are expected to adjust human relationship through listening and feedback by observers. Members with different knowledge, assumptions, values, and conflicting interests need to engage in dialogue to deepen their differences as a preliminary step to mutual understanding, rather than rushing to conclusions. Such flat and open dialogue can lead to cooperation that transcends vertical divisions.

BOX 13: Compliance risk management (conduct risk management)

Compliance risk management (conduct risk management) is integral to operational risk management. The conduct expected of financial institution is "first, to consider it their responsibility to meet the legitimate and reasonable expectations of their users, and to demonstrate this through their interactions with users, actions among financial institutions, and activities in the market." Conduct risk encompasses acts that adversely impact user protection, market integrity, and effective competition. Typical examples include market manipulation such as LIBOR fraud, conflicts of interest, insider trading, breaches of accountability to customers, and breaches of suitability principles.

In a narrow sense, compliance risk refers to violations of laws, regulations, and rules. However, even if no laws, regulations, or rules have been violated, an infringement of social norms constitutes conduct risk (compliance risk in a broader sense). Unlike operational risk under the Basel framework, conduct risk also applies when the firm does not directly incur losses, but when external stakeholders, such as users, do. For the firm, losses are indirectly

incurred in the form of materialized reputational risk.

From a compliance risk management (conduct risk management), a corporate culture that leans towards profit supremacy or authoritarianism is likely to cause violations of user protection. Therefore, a sound and open corporate culture is needed. Establishing such a risk management culture is crucial to ensure operational resilience. The FSA has already published a discussion paper on compliance risk management (conduit risk management)[34], as well as other documents containing examples and issues[35].

IV. Next steps

The operational resilience of each financial institution varies depending on its business type, size, risk appetite, and role within the financial system. Technological developments and changes in the external environment would also influence their practices and issues necessary to ensure operational resilience.

Therefore, the FSA does not intend to apply the viewpoints raised in this paper mechanically or uniformly or use them as a checklist in dialogue with financial institutions. Rather, taking into account the size and characteristics of each financial institution, the FSA will conduct surveys and engage in dialogue with management to thoroughly understand the current status of initiatives and issue awareness. This process will help identify issues needing attention to further advance these initiatives while considering the progress of international discussions. The FSA will then substantially promote the search for best practices among financial institutions by sharing good practices to these issues.

From the perspective of ensuring the stability of the financial system, the protection of users and financial service convenience, the FSA will continue engaging in constructive dialogue with a wide range of stakeholders and experts, including financial institutions. The FSA will also contribute to deepening international discussions.

[34] FSA (2018) "JFSA's Approach to Compliance Risk Management"
[35] FSA (2019) "Outline of Trends and Issues in Compliance Risk Management"