NRI

Rethinking operational resilience

Hitomi Kawahashi

11 April 2022

Iakyara vol.353

Nomura Research Institute, Ltd.

Executive Summary

Operational resilience is based on being prepared for unexpected events, recognizing that not all potential risks can be adequately addressed in advance. It is particularly useful in the context of bank system failures.

Hitomi Kawahashi
Senior Researcher
Financial Market & Digital Business Research Department

Japan's FSA issued a business improvement order to Mizuho Financial Group (MFG) in November 2021 in response to a series of eight system outages that inconvenienced customers over the preceding ten months. The recurring outages imply that financial institutions have deficiencies in terms of their (1) system risk management required to maintain stable system operations, (2) governance regime and/or (3) organizational culture. While MFG may be an outlier given the frequency of its system outages, we suspect that vulnerabilities in these three areas are common among all financial institutions pursuing digitalization.

Changing concept of operational risk management

The Basel capital framework classifies system risk as a type of operational risk[1]. How financial institutions think about and approach operational risk management has changed a lot in recent years with the emergence of the concept of operational resilience, defined by the Basel Committee on Bank Supervision (BCBS) as "the ability of a bank to deliver critical operations through disruption.[2]" The concept was originated by UK financial regulatory authorities[3] in 2018. In March 2021, the BCBS published Principles for Operational Resilience, the aim of which is to strengthen financial institutions' ability to absorb operational risk-related events (e.g., pandemics, cyber incidents, technology failures, natural disasters) that could cause systemically significant operational failures. Another factor behind the Principles for Operational Resilience's publication was a recognition that not all potential operational risk-related events can be prevented. Some risk events will occur despite doubly or even triply redundant precautions. The BCBS sees operational resilience as a new regulatory imperative behind capital and liquidity regulations.

Japanese banks have been placing priority on real-time processing in their

NOTE
1) The Basel Committee on Banking Supervision defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."
2) Principles for Operational Resilience (March 2021)
3) Specifically, the Bank of England, Prudential Regulation Authority and Financial Conduct Authority.

©2022 Nomura Research Institute, Ltd. All Rights Reserved.

core systems from the standpoint of not only their internal accounts but also customer service. Their systems have earned a reputation for reliability both in Japan and internationally. Japan being one of the world's most earthquake-prone countries, its banks were among the first in the world to build redundancy into their operational infrastructure as a precaution against natural disasters. Japanese banks' system risk management practices have long been predicated on their systems operating uninterruptedly. Prolonged system downtime did not enter into their risk management calculus. We surmise that one reason behind MFG's disorganized, slow response to its spate of system outages was that its IT staff and management were caught off guard when redundant safeguards failed to function as expected.

Operational resilience is based on expecting the unexpected. It recognizes that adequately addressing all potential risks in advance is impossible. In this sense, it is a major departure from the traditional approach of attempting to minimize the probability of unexpected events occurring. It also bears some similarity to reverse stress-testing, which involves identifying events that could lead to a certain predefined outcome (e.g., ¥xx billion capital impairment) and devising preventive/mitigative measures accordingly. The objective of such an approach is to eliminate bank executives' psychological aversion to entertaining the thought of events like critical-system outages.

Operational resilience entails a four-step process. The first step is to identify critical business processes and services from an operational resilience perspective. The second is to set tolerances for disruptions to each business process/service based on the maximum-duration the bank is willing to tolerate assumed disruptions. Third, the bank gauges its status quo against the tolerance set for each business process/service and devises measures and procedures to limit disruptions' impact to within the set tolerances. Lastly, the bank formulates a business continuity plan to continue operating and providing services even when a system is down. Business continuity planning means figuring out what the bank's capabilities are when certain business processes and/or services are interrupted.

How financial institutions have benefited from embracing operational resilience

Among financial institutions that have incorporated the concept of operational

©2022 Nomura Research Institute, Ltd. All Rights Reserved.

resilience into their operational risk management ahead of their Japanese counterparts, one benefit is that they are able to more efficiently allocate investments required for risk management. While financial institutions' regulatory compliance burden has increased in the wake of post-GFC regulatory tightening, operational risk's scope has become much more broad with the emergence of new risks such as novel forms of financial crime and conduct risk. This trend has in turn compounded the growing regulatory burden. More than a few financial institutions' CEOs were worried that if regulatory burden continued to grow, a major earnings squeeze would ensue to the potential detriment of their companies' business continuity. Since adopting operational resilience, however, they have started investing from the standpoint of not only preventing operational risks from materializing but also limiting resultant impacts to within predetermined tolerances in the event the risks do materialize. They have consequently been able to reduce redundancy investments they had previously been making to ensure that the operational risks never materialized.

A second benefit is that financial institutions have started to screen IT systems and business processes from a risk management standpoint while still in the development stage. They were previously more focused on project management (i.e., completing development on schedule) than on risk management when developing systems and business processes. An executive at a major financial institution told me that by virtue of adopting an operational resilience mentality, envisioning potential disruption scenarios and screening systems-under-development for flaws that increase the risk of those scenarios, his staff is now able to detect issues in the development stage that could give rise to future operational risk events. This approach has led to smoother rollouts of new services and products.

One challenge to adopting an operational resilience approach is that the conventional management mentality is not easy to change. Senior executives really do not want to think about critical-system outages or service interruptions. Nor do they have confidence in their ability to set tolerances. To dispel such psychological resistance, the Bank of England and UK Prudential Regulation Authority recommend changing the organizational culture as a prerequisite to strengthening operational resilience. For banks today, experimenting with new approaches without changing old ways of thinking is the biggest risk.

©2022 Nomura Research Institute, Ltd. All Rights Reserved.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.9 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.

For more information, visit https://www.nri.com/en

The entire content of this report is subject to copyright with all rights reserved.
The report is provided solely for informational purposes for our UK and USA readers and is not to be construed as providing advice, recommendations, endorsements, representations or warranties of any kind whatsoever.
Whilst every effort has been taken to ensure the accuracy of the information, NRI shall have no liability for any loss or damage arising directly or indirectly from the use of the information contained in this report.
Reproduction in whole or in part use for any public purpose is permitted only with the prior written approval of Nomura Research Institute, Ltd.

Inquiries to : Financial Market & Digital Business Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/fis/lakyara/

©2022 Nomura Research Institute, Ltd. All Rights Reserved.