FRB SOUND PRACTICES TO STRENGTHEN OPERATIONAL RESILIENCE AND CAPCO'S RESPONSE

By Michael Martinen, Managing Principal

On October 30, 2020, the Federal Reserve System's Board of Governors (FRB), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) issued an interagency paper titled Sound Practices to Strengthen Operational Resilience[1]. Bringing together industry standards and existing regulations, the publication is directed at large, complex domestic banking organizations[2] and advocates for a principles-based approach to enhance and bolster operational resilience.

The joint paper defines operational resilience as the "ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard," and highlights the identification of critical operations and core business lines as an essential prerequisite to an effective operational resilience strategy. The paper also stresses the mapping of interconnections and interdependencies across functions, business lines, and third parties, as this comprehensive mapping will inform a cohesive and adaptive operational resilience approach.

Following these identification and mapping exercises, the FRB, OCC, and FDIC promote the following principles regarding operational resilience:

1. GOVERNANCE

An effective governance structure is top-down, with the board of directors responsible for:

- Periodic review and approval of the firm's risk appetites and tolerance for disruption
- Appropriate allocation of resources to support operational resilience efforts
- Oversight of operational risk management across business lines, risk functions, and internal audit

And senior management for:

- Maintaining a detailed overview of the firm's structure to identify critical operations
- Ensuring the firm's areas remain within defined risk tolerances
- Implementing and maintaining information systems and controls which effectively support critical operations

Capco's Response: Restructure existing governance committees to incorporate an operational resilience component comprised of risk, operations, IT, and business continuity leaders to coordinate resiliency efforts across senior management, respective functions and third parties. This includes autonomy to make firm-wide operational resilience decisions and align resources accordingly. Leaders should leverage Capco's tailored-for-operational-resilience OODS framework and ensure resiliency strategies are broadly communicated and account for overall risk appetite and defined tolerance for disruption.

2. OPERATIONAL RISK MANAGEMENT

Firms must continue the ongoing identification, documentation, and Management of operational threats and vulnerabilities with the potential to disrupt critical operations. Close coordination with senior management is necessary to implement and maintain the controls, systems, and processes to accomplish the following:

- Identification and mitigation of operational risk exposures with a priority on critical operations and business services
- Ongoing programs for the assessment of control and procedure effectiveness
- Coordination across relative functions to appropriately document and address risk

[1] https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf

[2] The US guidance pertains to banks that have average total consolidated assets greater than or equal to: (a) $250 billion, or (b) $100 billion and have $75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets, or average off-balance sheet exposure.

The above should be supported by recurring review and challenge by internal audit, and lessons learned from previously experienced events or disruptions should be cataloged and incorporated into operational risk management practice.

Capco's Suggestion: Establish channels to leverage existing operational risk management processes and controls to develop resilience-focused incident scenarios and impact tolerances. Implement surveillance frameworks that assess the firm's risk exposure and control environment effectiveness on a quarter over quarter basis, using results to continuously refresh operational risk management and resiliency plans.

3. BUSINESS CONTINUITY MANAGEMENT

Maintain robust business continuity and crisis management plans that identify the people, facilities, and IT systems needed to uphold the delivery of critical operations during an incident or disruption. Business continuity management strategy should incorporate:

- Training and awareness programs enabling employees to respond to risk events effectively
- Ongoing business continuity plan testing, including considerations for IT systems and third parties
- Recovery and resolution plans, post-incident business impact analyses and transition plans for returning to business as usual (BAU)
- Maintenance of wide-scale remote access facilities and communication technology

Capco's Suggestion: Coordinate across the bank's critical functions to proactively develop continuity plans and crisis playbooks that are both scalable and adaptable given the nature and scope of an incident, considering both geographical outreach and interdependencies between the bank's functions. Continually run scenario analyses of potential risk events in independent and randomized combinations to note all gaps and potential vulnerabilities in critical operations.

4. THIRD-PARTY RISK MANAGEMENT

Assess risk exposure and operational resilience maturity of all third parties and contractors, especially when third parties support critical operations and business services. Effective management of third-party risk encompasses:

- Assess third party operational resilience through due diligence and on an ongoing basis
- Include expectations for maintaining operational resilience in all formal agreements
- Identify contingency service providers in the event a contractor is unable to support operations as a result of an incident or disruption

Capco's Suggestion: Third parties relied upon for the delivery of critical operations should be treated as in-house functions with the same level of governance, controls, and communications, which means developing and implementing an end-to-end third-party operational resilience framework with particular emphasis on areas exposed to heightened operational and cyber risk. Additionally, banks should maintain an inventory of potential third parties to which operations can be transferred or outsourced if a risk event impacts those already under contract.

5. SCENARIO ANALYSIS

Assess the firm's operational resilience across a wide range of severe but plausible scenarios to define, validate, and fine-tune impact tolerance limits. Incorporate results into recovery and resolution plans as well as business continuity management. Effective scenario analysis includes:

- Governance and independent review of the scenario development process
- Consideration for interconnections and interdependencies between the firm's business units, third party service providers, and information systems
- Backtesting against previous instances of operational risk events and disruptions

Capco's Response: Define resiliency-specific scenarios against macro-economic shifts from impacted industries, clients, and counterparties to understand how critical functions may pivot and reprioritize through different time periods. Use an inventory of scenarios to develop a digital representation of internal infrastructure, including visualizations of upstream, downstream, and cross-functional impacts of various incidents and disruptions. Draft playbooks defining response action plans to mitigate different scenario impacts. Scenarios should be evaluated on a real-time, dynamic cycle and incorporate lessons learned from internal and external events.

6. SECURE AND RESILIENT INFORMATION SYSTEM MANAGEMENT

Implement IT governance frameworks to ensure the proper implementation, use, and safeguarding of systems across business units and geographic locations. Ensure proper contingency plans and controls are in place to facilitate continued delivery of critical operations and information flow in the event of an incident or disruption. Sound practices for information system management also include:

- Ongoing programs to assess the effectiveness of controls and processes which ensure the overall security of IT systems and protection of data against destructive malware
- Continuous review of security measures involving emerging cyber threats and novel technologies
- Standardized tools and frameworks for monitoring cybersecurity preparedness

Capco's Response: Fortify the safety, soundness, and security of internal information management systems through a well-documented environment of IT protocols and controls. Review existing cybersecurity infrastructure and assess the capacity, bandwidth, and authentication mechanisms during BAU and remote work. Develop specific incident and breach management response plans to minimize data loss and protect the confidential firm and consumer information.

7. SURVEILLANCE AND REPORTING

Firms must comprehensively monitor operational risk exposure and potential disruptors of critical operations, aggregating relevant information and disseminating to the firm's board of directors and key stakeholders. Sound surveillance and reporting practices entail:

- Effective coordination and communication of risk appetite and tolerance for disruption
- Review and detection of activities posing risks to critical operations and business services
- Board and senior management reporting which includes sufficient data and information for suitable and timely decision-making

Capco's Response: Enhance existing reporting dashboards to incorporate real-time monitoring of operational risk exposures and emerging resiliency risks. Early warning of emerging issues or risks is key, as this informs actions that must be taken to ensure functions remain within their stated impact tolerances. Use relevant dashboard outputs to curate comprehensive and detailed reporting to the firm's board of directors and senior stakeholders, which will pinpoint areas in need of remediation and inform the continuous enhancement of existing controls and processes.

Implementing an effective operational resilience program is a significant undertaking requiring a cultural shift from reactive operational risk management to proactive management of emerging resiliency risks. Fortunately, many of the processes and functions needed are already up and running. The key is progressing from traditional governance constructs to data-driven frameworks that aggregate and interpret the above-outlined activities' data outputs. These predictive analytics should be embedded in the continuous review and scenario analysis processes, facilitating faster and more effective decision making to mitigate the impacts of incidents and disruptions before they materialize.

Contact us to learn more about the above guidance from the FRB, OCC, and FDIC, and our work managing end-to-end operational resilience transformations for global financial services institutions.

Michael Martinen, Managing Principal, michael.martinen@capco.com

So Jene Kim, Partner, so.jene.kim@capco.com

WWW.CAPCO.COM

CAPCO

JN_2655