Sound Practices to Strengthen Operational Resilience

Introduction

The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (the agencies) are issuing an interagency paper on *Sound Practices to Strengthen Operational Resilience* (sound practices). The sound practices seek to provide firms with ways to strengthen their operational resilience in the face of internal and external operational risks[1] that, left unchecked, could lead to a wide-scale disruption.

In recent years, firms have experienced significant challenges from a wide range of disruptive events including technology-based failures, cyber incidents, pandemic outbreaks, and natural disasters. While advances in technology have improved firms' ability to identify and recover from various types of disruptions, increasingly sophisticated cyber threats and growing reliance on third parties continue to expose firms to a range of operational risks. These operational risks underscore the importance for firms of all sizes to strengthen their operational resilience. While potential hazards may not be prevented, the agencies consider that a flexible operational resilience approach can enhance the ability of firms to prepare, adapt, withstand, and recover from disruptions and to continue operations.

Although operational resilience is important to all firms, the sound practices set forth in this paper are written for use by the largest and most complex domestic firms. This paper describes sound practices drawn from existing regulations and guidance for individual national banks, state member banks, state nonmember banks, savings associations, U.S. bank holding companies, and savings and loan holding companies 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.[2] This paper does not set forth any new regulations or guidance for these firms, but brings together the existing regulations and guidance in one place to assist in the development of comprehensive approaches to operational resilience. It also highlights the importance of operational resilience with respect to firms' critical operations and core business lines.

---

[1] As specified in 12 CFR 3.101 and 217.101 (Regulation Q), operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. This definition includes legal risk but excludes strategic and reputational risk.

[2] This includes U.S. domestic firms that are considered 1) Globally Important Systemic Bank Holding Companies, 2) Category II bank holding companies, 3) Category II savings and loan holding companies, 4) Category III bank holding companies, or 5) Category III savings and loan holding companies. It also includes GSIB depository institutions supervised by the OCC, Category II national banks and Federal savings associations, and Category III national banks and Federal savings associations (*see, e.g.*, 12 CFR 3.2 and 50.3; 12 CFR 324.2). It does not apply to U.S. intermediate holding companies.

While the sound practices prioritize the operational resilience of critical operations and core business lines of a firm and its material entities,[3] a firm also should identify and address the resilience of other operations, services, and functions for which a disruption could have a significant adverse impact on the firm or its customers as part of operational resilience planning.

Critical operations and core business lines are defined as follows:

i. Critical operations are those operations of the firm, including associated services, functions, and support,[4] the failure or discontinuance of which would pose a threat to the financial stability of the United States.[5]
ii. Core business lines are those business lines of the firm, including associated operations, services, functions, and support, that, in the view of the firm, upon failure would result in a material loss of revenue, profit, or franchise value.

Most firms to which this paper is directed already identify their critical operations and core business lines in their recovery or resolution plans.[6] These plans map out operational interconnections and interdependencies among a firm's material entities, across business lines, and with significant third parties. Accordingly, firms that are subject to recovery or resolution planning requirements can leverage relevant information in these plans for managing operational resilience.

Operational resilience is the *ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions*.[7] A firm that operates in a safe and sound manner is able to identify threats, respond and adapt to incidents, and recover and learn from such threats and incidents so that it can prioritize and deliver critical operations and core business lines, along with other operations, services and functions identified by the firm, through a disruption.

Sound Practices to Strengthen Operational Resilience

The sound practices outlined in this paper bring together existing regulations, guidance, and statements as well as common industry standards and provide a comprehensive approach that firms may use to strengthen and maintain their operational resilience. In this approach effective governance grounds the sound practices. Robust operational risk and business continuity management anchor the sound practices, which are informed by rigorous scenario analyses and

[3] A material entity is a subsidiary or foreign office of a firm that is significant to the activities of an identified critical operation or core business line, or is financially or operationally significant to the resolution of the firm.

[4] Associated services, functions, and support include management information services. These encompass a firm's comprehensive processes, supported by computer-based systems, that provide the information necessary for the firm's management, including systems and applications for risk management.

[5] As set forth in 12 CFR part 243—Resolution Plans (Regulation QQ)—Definitions. Not all firms subject to recovery or resolution plans have critical operations.

[6] See 12 CFR part 243 (Regulation QQ); 12 CFR part 30, Appendix E.

[7] The agencies note that there are several definitions of operational resilience used in the financial services sector, including those set forth by the National Institute of Standards and Technology (NIST), the Federal Financial Institutions Examination Council (FFIEC), and the Basel Committee on Banking Supervision (BCBS). The consistent theme in all of the definitions is the importance maintaining the ability to deliver operations through disruption from any hazard.

consider third-party risks. Secure and resilient information systems underpin the approach to operational resilience, which is supported by thorough surveillance and reporting.

Appendix A provides a separate collection of sound practices for managing cyber risk in recognition of its significance as an operational risk, and its technical nature. Appendix B provides a glossary of definitions used in these sound practices.

1. Governance

Effective governance helps ensure that firms not only operate in a safe and sound manner and comply with applicable laws and regulations, but also maintain operational resilience. In keeping with existing regulations and guidance, the practices outlined below promote effective governance.

a) The firm's board of directors approves and periodically reviews its risk appetite[8] for weathering disruption from operational risks,[9] at the enterprise level and for the firm's critical operations and core business lines. In setting the firm's risk appetite, the board of directors articulates the firm's tolerance for disruption considering its risk profile and the capabilities of its supporting operational environment[10] ("*tolerance for disruption*").[11]

b) The firm's board of directors works with senior management to confirm that operational resilience practices are led and staffed by individuals with relevant expertise, approve appropriate budgets and resources, and promote a culture of effective risk management.

c) The firm's board of directors oversees the firm's management of operational risk in its business line operations, its independent operational risk management function, and its independent internal (or external) audit function. Senior management is accountable for ensuring that each of these areas adheres to the firm's tolerance for disruption.

d) Senior management is accountable for maintaining a detailed, accurate, and regularly updated overview of the firm's organizational and legal structure that identifies the critical operations and core business lines of the firm and its material entities.

e) Senior management is accountable for developing, implementing, and managing effective and resilient information systems and controls, as appropriate, to maintain critical operations and core business lines consistent with the firm's tolerance for disruption.

---

[8] As described in 12 CFR part 30, Appendix D, risk appetite is defined as the aggregate level and types of risk the board and senior management are willing to assume to achieve the firm's strategic business objectives, consistent with applicable capital, liquidity, and other requirements and constraints. For operational resilience purposes, risk appetite statements reflect qualitative considerations and, as appropriate, quantitative measures.

[9] As described in 12 CFR 3.101 and 217.101 (Regulation Q), operational risks cover a range of events, which are categorized across event types comprising internal fraud; external fraud; employment practices and workplace safety; clients, products, and business practice; damage to physical assets; business disruption and systems failures, including those related to cyber; and execution, delivery, and process management.

[10] The firm's operational environment would include, for example, systems, processes, technical infrastructure, risk management capabilities, and expertise.

[11] A firm's tolerance for disruption generally is informed by existing regulations and guidance and by the analysis of a range of severe but plausible scenarios that would affect its critical operations and core business lines.

f) The internal (or external) audit function is responsible for independently assessing the design and ongoing effectiveness of the firm's operational resilience efforts.

2. Operational Risk Management

By identifying, managing, and mitigating operational risk exposures related to internal processes, people, systems, external threats, and third parties, a firm is able to strengthen its operational resilience. Effective operational risk management involves close engagement by the firm's senior management, business line operations, independent operational risk management function, and independent internal (or external) audit function. In keeping with existing regulations and guidance, the practices outlined below promote effective operational risk management.

a) The firm's senior management oversees the implementation of operational risk management processes, systems, and controls to identify and contain the scope of a disruption, mitigate its effects, and resolve the disruption consistent with the firm's tolerance for disruption.

b) The firm's business line operations management identifies and mitigates operational risk exposures in alignment with the firm's tolerance for disruption.

c) The firm's operational risk management function assesses the critical operations and core business lines of the firm and its material entities. It determines the extent of exposure to various operational risks the firm faces or forecasts and the firm's ability to recover from a disruption.

d) The firm's operational risk management function regularly reviews, tests, and updates internal controls relevant to the firm's critical operations and core business lines including those performed by third parties.

e) The firm's operational risk management function implements and maintains risk identification and assessment approaches that adequately capture business processes and their associated operational risks, including technology and third-party risks.

f) The firm's independent internal (or external) audit function provides a review and challenge of the firm's operational risk management function and assesses whether it is appropriately operating within the firm's tolerance for disruption.

g) The firm's operational risk management function works closely with its business continuity management and recovery or resolution planning functions with respect to operational resilience efforts.

3. Business Continuity Management

Business continuity plans consider market- and enterprise-wide stresses and idiosyncratic risks that can imperil the continuity of a firm's critical operations and core business lines or otherwise

have a broader impact on the financial system.[12] A firm that is subject to recovery or resolution planning requirements can leverage the information in these plans for business continuity management purposes. In keeping with existing regulations and guidance, the practices outlined below promote sound business continuity management.[13]

a) The firm's business continuity management incorporates business impact analysis,[14] testing, training, and awareness programs, as well as communication and crisis management policies.

b) The firm periodically reviews its business continuity plan to ensure contingency strategies remain consistent with current operations, risks and threats, its tolerance for disruption, and recovery priorities.[15] For a firm that performs payment, clearing, and settlement activities in critical financial markets, contingency strategies align with existing guidance.[16]

c) The firm tests business continuity plans, reviews the execution of tests, and improves plans by incorporating lessons learned. Business continuity tests and exercises incorporate dependencies of critical operations and core business lines on third parties. When possible, the firm participates in disaster recovery and business continuity testing with third parties associated with critical operations and core business lines.

d) The firm confirms that functional testing procedures for assessing the ability of a firm's IT systems to deliver minimum service capacity to critical operations and core business lines are consistent with the firm's business continuity objectives. The firm's business continuity management considers and incorporates scenarios in which service capacity and business continuity objectives cannot be met.

e) The firm identifies and manages the availability of personnel who are essential to the execution of the firm's critical operations and core business lines.[17] The firm has (an) alternate site(s) that has sufficient resources (including personnel), technology capabilities, and functionality

---

[12] See FFIEC Information Technology Examination Handbook booklet "Business Continuity Management," November 2019, which describes principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations.

[13] Guidance includes SR letter 03-9 and OCC Bulletin 2003-14 "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" (April 8, 2003) which outline practices for geographic diversity and resiliency of data centers and operations, as well as recovery and resumption time objectives and related testing standards for firms that perform payment, clearing, and settlement activities in critical financial markets. Per this guidance, the term recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption.

[14] See section III.A. "*Business Impact Analysis*" of the FFIEC Information Technology Examination Handbook booklet "*Business Continuity Management*," November 2019, which describes the business impact analysis process.

[15] See Sections II.A. "Board and Senior Management Responsibilities" of the *FFIEC Information Technology Examination Handbook* booklet "Business Continuity Management" November 2019.

[16] Refer to SR letter 03-9 and OCC Bulletin 2003-14 "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" (April 8, 2003).

[17] See Section IV.A.4 "Personnel" of the FFIEC *Information Technology Examination* Handbook booklet "Business Continuity Management" November 2019.

to execute the firm's critical operations and core business lines in the event of a disruption.[18] The alternate site(s) is (are) located at a sufficient geographical distance from the primary site and has (have) a distinct risk profile.

f) The firm's business continuity management includes remote-access contingencies that allow personnel to continue delivering the firm's critical operations and core business lines through a disruption.[19] The management of contingencies prioritize critical operations and core business lines and provide personnel adequate connectivity, communication, and collaboration tools, essential technology resources, and access to network systems. These contingencies incorporate transitioning personnel back to normal operations following the resolution of a disruption.[20]

g) The firm trains essential personnel who have responsibility for executing critical operations and core business lines to perform back-up roles should a disruption occur. The firm implements an operational resilience training and awareness program to evaluate the effectiveness of personnel-related business continuity arrangements and the program is improved as shortcomings are identified.

h) The firm's recovery or resolution planning, if applicable, is integrated into its governance and operating processes and is part of business-as-usual activities, including firm-wide risk management processes. In the context of operational resilience, recovery or resolution planning is understood as complementary to, and linked with, existing risk management and business continuity management processes.

i) The firm leverages information contained in its recovery or resolution plans, where applicable, to identify options to respond to a wide range of severe but plausible internal and external stress scenarios. The firm similarly leverages the identification of interconnections and interdependencies among critical operations and core business lines affiliates, subsidiaries, and third parties.

4. Third-Party Risk Management

In recent years, firms have made increasing use of third parties to deliver a variety of services, including those that are integral to critical operations and core business lines. Recognition of third-party risk is vital to operational resilience, especially if outsourcing arrangements involve entities that perform critical operations or core business activities. In keeping with existing regulations and guidance, the practices outlined below promote sound management of third-party risk.[21]

---

[18] See Section V.C "Facilities and Infrastructure" of the FFIEC *Information Technology Examination* Handbook booklet "Business Continuity Management", November 2019.

[19] The firm's operational risk management and independent internal (or external) audit functions also take into account remote-access and any other related conditions.

[20] See Section IV.A.4 "Personnel" of the FFIEC *Information Technology Examination* Handbook booklet "Business Continuity Management", November 2019.

[21] Federal Reserve SR 13-19 "Guidance on Managing Outsourcing Risk" (December 5, 2013); OCC Bulletin 2013-29 "Third Party Relationships: Risk Management Guidance" (October 30, 2013); Third Party Risk: Guidance for Managing Third Party Risk," FDIC FIL-44-2008 (June 6, 2008).

a) The firm identifies and analyzes third-party risk of critical operations and core business lines. It prioritizes third-party dependencies that are most significant to the firm and understands, manages, and mitigates its risks.

b) The firm establishes relationships with third parties through formal agreements.[22] The firm's manages and monitors the performance of third parties against its service requirements and its tolerance for disruption.

c) The firm periodically reviews reports of systems and controls and summaries of test results or other equivalent assessments of third parties. It establishes processes and benchmarks for monitoring a third party's ability to continue to deliver services during disruptions.[23]

d) The firm verifies that third parties have sound risk management practices and controls in place that serve to identify and mitigate hazards to operations and are consistent with the firm's tolerance for disruption.

e) The firm addresses key third-party concerns to the extent that these concerns affect the firm's operational resilience (e.g., through due diligence, contract negotiations, ongoing monitoring, and termination of contracts).

f) The firm identifies risks of third parties that provide it with public and critical infrastructure services, such as energy and telecommunications. The firm has processes to manage disruptions of these services and updates these processes as appropriate to stay within its tolerance for disruption.

g) The firm identifies other third parties that may be available to assist in the event its current third parties are unable to continue delivering services. The firm assesses the substitutability of third parties that provide services supporting the firm's critical operations and core business lines including the possibility of bringing a service back in-house.

5. Scenario Analysis

Scenario analysis helps a firm to develop, validate, and calibrate a firm's tolerance for disruption. Firms may integrate the analysis with disaster recovery and business continuity management for use in assessing operational resilience. In keeping with existing regulations and guidance, the practices outlined below promote effective scenario analysis.[24]

---

[22] 12 U.S.C. 1867(c)(2) requires firms to notify the Agencies of service relationships.

[23] FFIEC Interagency Statement on Pandemic Planning (March 6, 2020) and FFIEC Information Technology Examination Handbook booklet "Business Continuity Management", November 2019.

[24] The Interagency Guidelines Establishing Standards for Safety and Soundness, adopted pursuant to Section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p-1), set forth standards for institutions to have systems that provide for an effective risk assessment that identifies the nature, scope, and risk of its activities, products, and balance-sheet components. Depository institutions should refer to the Interagency Guidelines adopted by their primary federal regulator as follows: For national banks and federal savings associations, Appendix A to 12 CFR part 30; for state member banks, Appendix D-1 to 12 CFR part 208; and for state nonmember banks, state savings associations, and insured state-licensed branches of foreign banks, Appendix A to 12 CFR part 364. See also SR 15-19 Federal Reserve Supervisory Assessment of Capital Planning and Positions for Large and Noncomplex Firms, Appendix G (December 18, 2015).

a) Operational risks identified by the firm's operational risk management function, independent internal (or external) audit function, business continuity management, and recovery or resolution planning activities should be incorporated, as applicable, into severe but plausible scenarios affecting the firm's critical operations and core business lines. The firm designs the scenarios so that they may be used to test the firm's tolerance for disruption.

b) The firm maintains a robust governance framework and independent review function to oversee the integrity and consistency of the scenario development process.

c) In designing scenarios, the firm leverages both the mapped interconnections and interdependencies of its critical operations and core business lines including its third-party risks, set forth in its recovery or resolution plans, as well as relevant business impact analyses.

d) The firm uses scenario analysis to back-test against past instances of severe disruptions that have arisen from various disruptions. The results of back-testing are used to refine scenarios and increase their effectiveness for future.

e) The firm identifies potential risk transmission channels, concentrations, and vulnerabilities by analyzing the interconnections and interdependencies within and across its critical operations and core business lines considering third-party risks. The information that is obtained from these analyses informs the firm's tolerance for disruption.

6. Secure and Resilient Information System Management

Secure and resilient information systems underpin the operational resilience of a firm's critical operations and core business lines. The appropriate implementation, use, and protection of information systems can help a firm identify and detect risks to operational resilience. They also enhance its ability to withstand disruptions or failures and facilitate the flow of information to enable effective decision-making during a disruption. In keeping with existing regulations and guidance, the practices outlined below promote secure and resilient information systems.[25] Additional sound practices on cyber risk management are provided in Appendix A.

a) Information systems, including elements that depend on third parties, supporting the firm's critical operations and core business lines are subject to robust risk identification, protection, detection, and response and recovery programs that are regularly tested. Information systems incorporate appropriate situational awareness and provide management with relevant information on a timely basis.

b) The firm routinely applies and evaluates the effectiveness of processes and controls to protect the confidentiality, integrity, availability, and overall security of the firm's data and information systems.

c) The firm establishes controls to safeguard the integrity and availability of critical data against the impact of destructive malware, including ransomware, or other similar threats. Recovery

[25] Consistent with FFIEC Information Technology Examination Handbook, November 15, 2019, revised December 12, 2019.

from such incidents may include use of protocols for secure, immutable, off-line storage of critical data.

d) The firm reviews information systems and controls on a regular basis against common industry standards and best practices. The firm also regularly reviews and updates its systems and controls for security against evolving threats including cyber threats and emerging or new technologies.

e) The firm may benefit from use of a standardized tool that is aligned with common industry standards and best practices to assess its cybersecurity preparedness as described in Appendix A.

7. Surveillance and Reporting

Operational resilience entails ongoing surveillance and reporting of operational risks and dissemination of that information to the board of directors and relevant stakeholders across the firm. In keeping with existing regulations and guidance, the practices outlined below promote sound surveillance and reporting.[26]

a) The firm identifies and monitors ongoing exposure to operational risk relative to its risk appetite and tolerance for disruption. The firm establishes and maintains appropriate communication and coordination procedures to inform all relevant areas of the firm's ongoing exposures.

b) The firm detects in a timely manner anomalous activity that could lead to a disruption affecting the firm's critical operations and core business lines, and it assesses the potential impact of the activity together with the effectiveness of protective measures.

c) The firm conducts continuous surveillance and reporting to senior management and the board of directors that provides sufficient data and information for timely and appropriate decisions regarding measures to respond to a disruption.

[26] See Section IV.B "Communications" of the FFIEC *Information Technology Examination* Handbook booklet "Business Continuity Management", November 2019.

Appendix A

Sound Practices for Cyber Risk Management

To manage cyber risk and assess cybersecurity preparedness of its critical operations, core business lines and other operations, services, and functions firms may choose to use standardized tools that are aligned with common industry standards and best practices. Some of the tools that firms can choose from include the FFIEC Cybersecurity Assessment Tool, the National Institute of Standards and Technology Cybersecurity Framework (NIST), the Center for Internet Security Critical Security Controls, and the Financial Services Sector Coordinating Council Cybersecurity Profile.[27] While the agencies do not endorse the use of any particular tool, Table 1 below presents a collection of sound practices for cyber risk management, aligned to NIST and augmented to emphasize governance and third-party risk management.

Table 1: Sound Practices for Cyber Risk Management

Categories	Attributes
Governance	The firm's risk appetite and tolerance for disruption reflect the scope and level of cyber risk the firm is willing to accept or avoid for its critical operations and core business lines.[28]
	The firm establishes, implements, and manages cyber risk management processes for its critical operations and core business lines and integrates them into operational risk management processes.
	The firm has established cybersecurity processes to support operating within its risk appetite and tolerance for disruption.
	The firm has designated roles and responsibilities for cyber risk management, including an individual responsible for cybersecurity for the firm.
	The firm has a cybersecurity program that implements, monitors, and updates existing processes. The cybersecurity program is continually monitored and improved.
	The firm's independent risk management and independent internal (or external) audit function provides for appropriate oversight of the cybersecurity program.
Identification	The firm identifies and manages data, personnel, devices, systems, third parties and facilities that enable its critical operations and core business lines.
	The firm understands the cybersecurity risks to its critical operations and core business lines, and their underlying data, personnel, devices, systems, third parties, and facilities associated with them.

[27] See FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness, August 26, 2019, (https://www.ffiec.gov/press/pr082819.htm).

[28] The firm's operational risk appetite statements are discussed in the governance section of the operational resilience sound practices.

Protection	The firm limits access to physical and logical assets and related facilities for its critical operations and core business lines to authorized users, processes, and devices, and manages access consistent with the assessed risk of unauthorized access to activities and transactions that require authorization.
	The firm provides cybersecurity awareness education especially to personnel engaged in the operations of critical operations and core business lines, including those from third parties and adequately trains them to perform their information security-related duties and responsibilities consistent with related processes and agreements.
	The firm manages information and data consistent with its risk appetite and tolerance for disruption to protect the confidentiality, integrity, and availability of data and systems.
	The firm maintains security processes that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities; and processes and uses them to manage protection of information systems and assets.
	The firm encrypts data used in the delivery of critical operations and core business lines. The firm protects data at "rest" and "in transit" commensurate with the criticality and sensitivity of the information.
	The firm creates backups of critical data and regularly tests those backups for completeness and reliability.
	The firm disposes critical assets in a secure manner in order to prevent unauthorized recovery of sensitive information.
	The firm manages configuration baselines that incorporate its information systems resilience requirements. The management of configuration changes causes minimal disruption to the delivery of critical operations and core business lines.
	The firm maintains and repairs industrial control[29] and information system components consistent with policies and procedures.
	The firm's information systems architecture for critical operations and core business lines incorporates the firm's cyber resilience requirements and is secure by design. The firm also accounts for interdependency, interconnectivity, scale, and complexity risks.
	The firm has and enforces defined processes for technology acquisition, development, testing, and integration that incorporate the firm's resilience requirements throughout the processes' lifecycles.
	The firm upgrades or replaces information system components before technical support is no longer available from the developer, vendor, or manufacturer.
	Technical security solutions are used to manage the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

[29] Firms often use industrial controls systems to automate heating, ventilation, and cooling systems, power systems, etc. According to NIST, industrial control systems are information systems used to control industrial processes such as manufacturing, product handling, production, and distribution. https://csrc.nist.gov/glossary/term/industrial_control_system.

Detection	Anomalous activity is detected in a timely manner and the potential impact (including financial impact) of anomalous events is analyzed and understood.
	Information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection processes and procedures are maintained and tested to ensure timely action is taken in response to anomalous events.
Response	Response processes and procedures are executed and maintained for timely response to detected cybersecurity incidents.
	The firm coordinates response activities with internal and external stakeholders, as appropriate, including external support from regulatory and law enforcement agencies.
	The firm conducts analysis to ensure effective response and to support recovery activities.
	The firm performs activities to prevent expansion of a disruption, mitigate its effects, and resolve the incident.
	The firm improves response activities by incorporating lessons learned from current and previous detection/response activities.
Recovery	The firm executes and maintains business continuity and disaster recovery plans, processes and procedures to support timely restoration of systems or assets affected by cybersecurity incidents.
	The firm improves recovery plans and processes by incorporating lessons learned into future activities.
	The firm coordinates restoration activities with internal and external parties such as internet service providers, owners of compromised systems, other incident response teams, and vendors.
Third-party risk management	The firm manages the risks to its critical operations and core business lines, and monitors the effectiveness of controls associated with them, regardless of whether the firm performs the activity internally or through a third party.
	The firm engages in robust planning and due diligence to identify risks related to third parties and establishes processes to measure, monitor, and control the risks associated with them. The process for risk identification and monitoring controls effectiveness may include testing or auditing of security controls with the third party.
	Contracts between the firm and third parties are drafted to define clearly which party is responsible for configuring and managing system access rights, configuration capabilities, and deployment of services and information assets.
	Relationships with third parties include sound risk management practices to identify and mitigate hazards. The firm employs controls to verify that resilient operational processes are in place at the third party and consistent with the firm's internal standards.
	The firm has processes for validating that third-party systems used for delivering critical operations and core business lines will be operational during disruptions or able to return to operation in accordance with the firm's tolerance for disruption.

Appendix B

Glossary of Definitions

Business continuity management. Refers to measures that promote the continuous operation of a firm or financial market in the event of a disruption or crisis.

Core business lines. Those business lines of the firm, including associated operations, services, functions and support, that, in the view of the firm upon failure would result in a material loss of revenue, profit, or franchise value.

Critical operations. Those operations of the firm, including associated services, functions and support, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

Cyber incident. An incident that jeopardizes the cybersecurity of an information system or the information the system processes, stores or transmits or that violates cybersecurity procedures.

Cyber risk. Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a system via electronic means from the unauthorized access, use, disruption, modification, or destruction of the system.[30]

Essential personnel. Essential personnel are individuals, including those from third parties, whose availability is necessary for the delivery of a firm's critical operations and core business lines.

Information systems. A set of applications, services, information technology assets or other information-handling components, which includes the operating environment.

Management information systems. A firms' comprehensive processes, supported by computer-based systems that provide the information necessary to manage the firm. These include systems and applications for risk management.

Material entity. A subsidiary or foreign office of a firm that is significant to the activities of an identified critical operation or core business line, or is financially or operationally significant to the resolution of the firm.

Operational resilience. The ability to deliver operations, including critical operations and core business lines through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.

Operational risk. The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

[30] As defined by the National Institute of Standards and Technology (https://csrc.nist.gov/glossary/term/cyber_risk).

Risk appetite. The aggregate level and types of risk the board and senior management are willing to assume to achieve a firm's strategic business objectives, consistent with applicable capital, liquidity, and other requirements and constraints.

Third parties. Entities that have a business arrangement with a firm. Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the firm has an ongoing relationship or may have responsibility for the associated records.

Tolerance for disruption. Tolerance for disruption is determined by a firm's risk appetite for weathering disruption from operational risks considering its risk profile and the capabilities of its supporting operational environment. A firm's tolerance for disruption is informed by existing regulations and guidance[31] and by the analysis of a range of severe but plausible scenarios that would affect its critical operations and core business lines.

[31] Such as FRB SR Letter 03-9 and OCC Bulletin 2003-14 "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" (April 8, 2003).