PROTECHT

WHITE PAPER

Interagency guidance on sound practices to strengthen operational resilience.

An overview of U.S. interagency guidance SR 20-24 on operational resilience.

Executive summary.

"Operational resilience is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard."

SR 20-24

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) have issued an interagency paper on Sound Practices to Strengthen Operational Resilience (sound practices).

These sound practices bring together the existing regulations and guidance in one place. This will assist in the development of comprehensive approaches to operational resilience, especially with respect to critical operations and core business lines where risks could lead to a wide-scale disruption.

Critical operations are defined as those that if disrupted, would pose a threat to the financial stability of the United States. Core business lines are defined as those that if disrupted, would result in significant loss of revenue, profit, or franchise value.

Although operational resilience is important to all firms, the sound practices set forth in the paper are written for use by the largest and most complex domestic firms. Examples include 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.

This white paper provides an executive summary of the report, offering insights critical for busy operational risks managers and covering topics including:

What to do:

- Governance
- Operational risk management
- Business continuity management
- Third-party risk management

How to do it:

- Scenario analysis
- Information system management
- Surveillance and reporting
- Cyber risk management

PROTECHT

Contents

01

What to do.

The first part of the guidance considers the broad topic of what operational resilience actually consists of and how that can be broken down into different kinds of risk management practice.

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. A firm's board of directors should be involved in the governance of operational resilience in the following ways:

- Approve and periodically review the firm's risk appetite considering its risk profile and the capabilities of its supporting operational environment.
- Confirm that operational resilience practices are led and staffed by experts, approve budgets, and promote a culture of effective risk management.
- Oversee the firm's management of operational risk in business line operations, operational risk management function, and audit function.

Senior management should be accountable for:

- Maintaining and updating the firm's organizational and legal structure to identify critical operations and core business lines.
- Developing, implementing, and managing risk management and information systems and controls to adhere to the firm's tolerance for disruption.

In addition, the internal or external audit function must be responsible for independently assessing the effectiveness of the firm's operational resilience efforts.

"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."

Operational risk management

The firm's senior management must oversee operational risk management activities that include identifying and containing a disruption, mitigating its effects, and resolving the disruption. Business line operations management identifies and mitigates operational risk exposures in alignment with the firm's tolerance for disruption.

Operational risk management staff have several roles, including:

- Determining the extent of exposure to operational risks and the firm's ability to recover from a disruption.
- Reviewing, testing, and updating internal controls including those completed by third parties.
- Implementing and maintaining risk identification and assessment approaches.
- Working closely with business continuity management and recovery or resolution planning functions with respect to operational resilience efforts.

Independent internal or external audit staff assesses whether the operational risk management function is operating within the firm's tolerance for disruption.

Business continuity management

Business continuity plans consider the firm's risks that can affect its ability to continue to operate even in the face of disruptions. Firms that are subject to recovery or resolution planning requirements can use those plans as a basis for business continuity management. The following issues should be addressed to create sound business continuity management.

- Including processes for business impact analysis, testing, training, and awareness programs along with communication and crisis management policies.
- Reviewing the business continuity plan regularly to ensure that contingency strategies are effective in the light of changes in operations, risk, threats, tolerance for disruption, and recovery priorities.
- Conducting tests of business continuity plans, including third party readiness, and updating plans based on results.
- Confirming that functional testing procedures for IT systems are consistent with business continuity objectives. Ensuring that some tests gauge effectiveness if service capacity and business continuity objectives can't be met.
- Ensuring that personnel who are essential to the firm's critical operations and core business lines are available and that alternate sites are adequately staffed and provisioned to provide backup. Alternate sites should be located in areas that have different risk profiles from the primary site.
- Ensuring the availability of remote-access contingencies for critical operations and core business lines.
- Implementing and updating training for essential personnel responsible for critical operations and core business lines to perform back-up roles if a disruption occurs.
- Integrating recovery or resolution planning into governance and operating processes. Linking operational resilience and recovery or resolution planning to existing risk management and business continuity management processes.
- Using recovery and resolution plans to respond to severe but plausible internal and external stress situations.

Third-party risk management

> *"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."*

Recognition of third-party risk is vital to operational resilience, especially if outsourcing arrangements involve entities that perform critical operations or core business activities. Promoting sound management of third-party risk includes the following:

- Identifying, analyzing, and mitigating third-party risks related to critical operations and core business lines.
- Using formal agreements to establish relationships with third parties.
- Establishing processes and benchmarks for monitoring a third party's ability to operate during disruptions. Periodically reviewing third-party reports and tests.
- Verifying that the third party's risk management practices correspond to the firm's tolerance for disruption.
- Using things such as due diligence, contract negotiations, ongoing monitoring, and contract termination to address third-party concerns if they affect operational resilience.
- Using processes to manage risks and disruptions of public and critical infrastructure services provided by third parties.
- Identifying in-house alternatives or third parties that can assist in the event that existing third-party services become unavailable.

02

How to do it.

The second part of the guidance deals with the more specific ways in which regulated entities can go about managing their operational resilience risks, by ensuring that they carry out regular and robust scenario analysis, that they follow best practice in managing information systems securely, that all processes are monitored and reported on a timely and sufficient basis, and finally by considering some more detailed aspects of cybersecurity.

Scenario analysis

Scenario analysis helps a firm to develop, validate, and calibrate a firm's tolerance for disruption. Scenario analysis practices can include:

- Incorporating operational risks identified by any operational risk management process into plausible scenarios to test the firm's tolerance for disruption.
- Using governance and independent review to ensure the integrity and consistency of the scenario development process.
- Using mapped interconnections and interdependencies from recovery or resolution plans, including third-party risks, and business impact analyses when designing scenarios.
- Using scenario analysis to back-test past instances of severe disruptions to refine the effectiveness of scenarios in the future.
- Analyzing the interconnections and interdependencies among critical operations and core business lines considering third-party risks to help establish the firm's tolerance for disruption.

Secure and resilient information system management

The appropriate implementation, use, and protection of information systems can help a firm identify and detect risks to operational resilience. In addition, information systems help the firm withstand disruptions and facilitate the flow of information to improve decision-making during a disruption. The following practices promote secure and resilient information systems.

- Subjecting information systems that support the firm's critical operations and core business lines to robust risk identification, protection, and response and recovery programs that are tested regularly.
- Evaluating the effectiveness of processes and controls to protect the confidentiality, integrity, availability, and overall security of the firm's data and information systems.
- Establishing controls to protect critical data against malware, ransomware, and similar threats that may include off-line storage of critical data.
- Reviewing information systems and controls on a regular basis to update based on industry standards, best practices, evolving threats such as cyber threats and emerging or new technologies.

Surveillance and reporting

Ongoing surveillance and reporting of operational risks is a key part of operational resilience. The results of that reporting should be disseminated to the board of directors and all stakeholders. Sound surveillance and reporting should consist of:

- Monitoring ongoing exposure to operational risks as compared to the firm's risk appetite and tolerance for disruption. The outcome should be communicated to all relevant stakeholders.
- Detecting anomalous activity in a timely manner and assessing the potential for it to disrupt the firm's critical operations and core business lines, and the effectiveness of protective measures.
- Reporting sufficient data and information to senior management and the board of directors, allowing them to make timely decisions on how to respond to a disruption.

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.

The agencies do not endorse any particular tool, but options 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.

The report contains an appendix that lists sound practices for cyber risk management, aligned to NIST and augmented to emphasize governance and third-party risk management. The following categories are covered:

- **Governance**: Addresses the need for specific governance activities to incorporate cyber risk management into the firm's overall risk management processes.
- **Identification**: Reinforces the need to identify and maintain data, personnel, devices, systems, third parties and facilities that support critical operations and core business lines, and the risks they face.
- **Protection**: Addresses sound protection activities, including protection for facilities, data, and systems architecture. Also lists requirements for cyber security training within the firm.
- **Detection**: Identifies requirements for timely detection of anomalous activity.
- **Response**: Identifies requirements for ensuring an appropriate response to cyber threats.
- **Recovery**: Identifies requirements for sound recovery plans and processes.
- **Third-Party Risk Management**: Identifies requirements for managing risks posed by third parties.

03

Conclusions and next steps for your organization.

Sound Practices to Strengthen Operational Resilience is intended to help firms stand up to the significant challenges that have appeared in recent years. Technology failures, pandemics, natural disasters, increases in the number and sophistication of cyber threats, and our growing reliance on third parties have all played a part in making operational resilience a critical topic for all firms.

This report is an excellent tool for operational risk managers to use in ensuring their firms can survive and thrive regardless of the threats that come their way.

Read the complete guidance on the Federal Reserve site.

Another important piece of regulatory guidance that should sit alongside SR 20-24 on your bookshelves is the U.S. interagency guidance SR 23-4 on managing risk in third-party relationships.

Interagency guidance on managing risk in third-party relationships.

SR 23-4 offers guidance designed to offer banks sound principles for assessing and managing the risks associated with third-party relationships including but not limited to those with outsourced service providers, independent consultants, and merchant payment processing services. It also provides a comprehensive framework for safely and effectively navigating such relationships.

If you'd like to find out more about SR 23-4, then Protecht has a companion white paper to this one which summarizes the guidance and what it means for your business.

Download it now

You can also check out the following operational resilience and related resources available from Protecht:

The complete guide to achieving operational resilience

Operational resilience is an organization's overall ability to deliver important business services when disruptive change happens. The rise in the frequency and magnitude of major shocks and attention from financial services regulators have placed operational resilience firmly in the spotlight.

The concept includes, but also goes beyond, the concepts of disaster recovery and business continuity. Rather than just allowing for recovery, operational resilience focuses on prevention and robustness to minimize the likelihood of recovery being required.

Download this eBook for a detailed look at operational resilience, to learn exactly what makes it different from disaster recovery and business continuity, and to learn how you can develop your own operational resilience capability and integrate it with your ERM framework.

Download it now

Other resilience and operational risk eBooks

Cyber risk management: The art of prevention, detection and correction.

This eBook provides practical strategies for executives, risk managers, and cyber security professionals to effectively measure, quantify, treat, and control cyber risk within their organisations.

Download it now

Information technology risk management.

Find out what information technology risk is, why it matters, why it's different from cyber risk, and why it's not just a concern for the IT department.

Download it now

Vendor risk management.

This eBook provides a detailed step-by-step guide to the stages required to build an effective vendor risk management program.

Download it now

Operational resilience and business continuity management in Protecht ERM

Prove your resilience.
Progress your business.

Prepare, withstand, recover and adapt. Ensure that your operational resilience and business continuity management processes are able to support your customers and meet your regulatory requirements.

Find out more and book a demo on our website:

Find out and book now

ABOUT PROTECHT

Redefining the way the world thinks about risk.

For over 20 years, Protecht has redefined the way people think about risk management. We help companies increase performance and achieve strategic objectives through better understanding, monitoring and management of risk.

We provide a complete solution comprised of world class risk management, compliance, training and advisory services to businesses, regulators and governments across the world.

With our flagship SaaS platform you can dynamically manage all your risks in a single place: risks, compliance, incidents, KRIs, vendor risk, IT and cyber risk, internal audit, operational resilience, BCP, health and safety, and more.

We're with you for your full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

NORTH AMERICA

+1 (833) 328 5471
1110 N Virgil Ave
PMB 95227
Los Angeles, CA 90029
United States

EUROPE, THE MIDDLE EAST & AFRICA

+44 (0) 20 3978 1360
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

AUSTRALIA & ASIA PACIFIC

+61 (0) 2 8005 1265
Level 8
299 Elizabeth St.
Sydney NSW 2000
Australia

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com