FS-ISAC

Fundamentals of Operational Resilience

Version 0.1

PREFACE

The global financial system is ever more complex and interconnected. Firms have been and will continue to operate in a challenging, ever-changing risk environment and future risks may not be the same as past disruptions. FS-ISAC's mission is to advance cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve. In support of this mission, FS-ISAC will produce and publish a series of public Operational Resilience guides that will cover the fundamentals of building an operational resilience program.

This guide is the first in the series and aims to introduce what operational resilience is, why it is critical for financial firms, and fundamental principles for building an operational resilience program. For clarification of this guide, Appendix A will define core words utilized in both this guide and future guides that will be released.

INTRODUCTION

Operational resilience is increasingly important for financial firms given the financial sector's growing interdependence and reliance on third-party service providers, information and operational technology, and infrastructure that is outside of the control of the company. This complex, highly networked ecosystem brings new risks that we must identify, assess, and manage.

It is essential for organizations to understand their risk landscape, internal/external interconnections and dependencies, internal deficiencies, continuity plans, and risk management plans to prevent as well as limit impacts during a disruption.

Operational resilience is a broad conceptual framework encompassing several traditional activities, such as business continuity and risk management, to ensure the company can adapt to changes in the risk landscape and continue to operate its important business services during a disruptive event.

The Bank for International Settlements defines operational resilience as "the ability to deliver critical operations through disruption. This ability enables organizations to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption."[1]

The following fundamental principles provide an introduction to building an operational resilience program within a financial services Organization. These principles are a culmination of principles described in operational resilience papers from the Federal Reserve, the Bank of International Settlements, and the Bank of England. These principles are designed to provide a foundation on which greater research may be needed. Companies should view these principles as a starting point on which to build and customize depending on their size, complexity, and role in the financial sector ecosystem.

1. Basel Committee on Banking Supervision. "Principles for Operational Resilience." The Bank for International Settlements. The Bank for International Settlements, August 6, 2020.

FUNDAMENTAL PRINCIPLES OF OPERATIONAL RESILIENCE PROGRAMS

Building an effective operational resilience program may include the following fundamental principles:

1 Understand your Critical Operations[2]

The identification of critical operations and the internal/external critical systems and processes on which they rely.

The Bank of International Settlements describes critical operations as "Any activity, function, process, or service, the loss of which would be material to the continued operation of the financial industry participant, financial authority, and/or financial system concerned."[3] It may be of benefit for organizations to determine both critical operations as well as the interdependencies to which these critical operations rely on. Interdependencies are to be considered "interconnections between internal and external systems based on direct relationships between the processes or indirect relationships arising from the activities of financial institutions in multiple systems and broader commonalities."[4] Interdependencies can be identified by mapping the interconnectedness of processes and functions. Identifying interdependencies may help an organization spot areas of weakness or understand the cascading impacts that may be caused to critical operations from non-critical components.

2 Understand your Risk & Threat Landscape

The identification of both risks and threats to critical operations may be of benefit to each organization to ensure they have the information necessary to establish plans and practices that protect against and mitigate disruption.

In order to create feasible and effective response plans, it is essential that organizations understand their risk and threat landscape. This is to ensure that the creation of response plans account for current hazards and dangers that organization may face. By understanding the risk and threat landscape, an organization may be able to better develop a plan that accounts for already known areas of concern. To begin mapping the risk and threat landscape, organizations may communicate with internal and external groups such as cyber security teams, information sharing bodies and/or government partners that may provide them with information on potential or current hazards. Additionally, it may be in the best interest of an organization to maintain an internal inventory of assets (both physical and digital), threats, and event classes.[5] This will assist organizations in maintaining a list of possible internal vulnerabilities or weak points as well as establish plans and practices that protect all assets.

3 Develop a Risk-Based Approach to Protection of Critical Operations

The establishment of risk and impact tolerance that are commiserate with the boards risk appetite for critical operations.

2. Critical operations are to be seen as conceptually similar to what some organizations, such as the Bank of England, may refer to as "important business services"

3. Basel Committee on Banking Supervision. "High-Level Principles for Business Continuity." The Bank for International Settlements, August, 2006.

4. This definition is based on the definition of Interdependency utilized by the Bank of International Settlements. Basel Committee on Payment and Settlement Systems "A Glossary of Terms Used in Payments and Settlement Systems." The Bank for International Settlements.

5. Federal Financial Institutions Examination Council. "FFIEC Information Technology Examination Handbook." Federal Financial Institutions Examination Council., November 2015.

When developing a risk-based approach in an effort to protect critical operations, organizations may want to consider the following: strategic risk, compliance risk, and reputational risk. During this time, it is essential that the organization's board remains engaged throughout the process. This may provide management with a more comprehensive view that allows for the creation of controls and plans that account for potential hazards as well as assists in prioritizing risks. A risk-based approach also provides organizations with the ability to create reasonable and feasible preventative measures commensurate with the level of risk posed as well as the risk appetite of the board.[6]

4 Develop Response Plans

The creation of response plans is essential to ensuring a more organized and coordinated response to incidents and crises. These response plans may account for past events and exercises that may dictate necessary changes or process standards that need to occur in an incident.

Response plans may identify:

- Areas such as critical operations, interdependencies (both internal and external), and internal decision making processes.
- Key members and teams within the organization as well as their expected roles and responsibilities during an incident.
- Lessons learned from previous incidents or exercises.

Additionally, response plans may be reviewed and updated on a regular basis as plans are tested in exercises or utilized in incidents that showcase deficiencies.

5 Conduct Exercises

Conduct exercises that may test several components of incident response both internally and/or externally, including but not limited to response plans, frameworks, processes, communication expectations, and organization coordination.

Organizations may consider running exercises on a regular basis to ensure their methods and processes for addressing an incident are feasible, effective, and reasonable. These exercises may simulate severe, but plausible scenarios that trigger internal and/or external processes for incident response.[7]

6 Implement Effective Governance

Establish effective governance for both internal and external partners to ensure they operate and develop enterprise-wide plans that comply with applicable laws and regulations, are efficient, and can be executed in a safe and sound manner.[8]

The Board of Directors and senior management may be useful resources for effective enterprise-wide governance. The Board of Directors may set the risk appetite for the organization. The risk appetite may drive decisions regarding tolerance for disruptions and response plans. This determination will be a vital piece in determining operational risks. Senior management may be responsible for ensuring feasibility, proper implementation, and resource allocation needed to carry out plans.

6. Financial Action Task Force. "Guidance for a Risk-Based Approach." FATF/OECD, October 2014.

7. Basel Committee on Banking Supervision. "Principles for Operational Resilience." The Bank for International Settlements. The Bank for International Settlements, August 6, 2020.

8. The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. "Sound Practices to Strengthen Operational Resilience." The Federal Reserve, November 2, 2020.

APPENDIX A: TERM LIBRARY

Critical Operations: Any activity, function, process, or service, the loss of which would be material to the continued operation of the financial industry participant, financial authority, and/or financial system concerned. [9]

Event Class: Categories of events such as natural disasters, cyber events, and insider abuse or compromise.[10]

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.[11]

Interdependencies: Interconnections between internal and external systems based on direct relationships between the processes or indirect relationships arising from the activities of financial institutions in multiple systems and broader commonalities.[12]

Operational Resilience: The ability to deliver critical operations through disruption. This ability enables organizations to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption.[13]

Operational Risks: The risk of failure or loss resulting from inadequate or failed processes, people, or systems.[14]

Risk: The potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings, capital, or reputation.[15]

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.[16]

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.[17]

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[18]

9. Basel Committee on Banking Supervision. "High-Level Principles for Business Continuity." The Bank for International Settlements, August, 2006.

10. Federal Financial Institutions Examination Council (FFIEC). "Information Technology Examination Handbook." Federal Financial Institutions Examination Council (FFIEC), November, 2015.

11. Computer Security Resource Center. "Glossary." National Institute of Standard and Technology.,csrc.nist.gov/glossary.

12. This definition is based on the definition of Interdependency utilized by the Bank of International Settlements. Basel Committee on Payment and Settlement Systems "A Glossary of Terms Used in Payments and Settlement Systems." The Bank for International Settlements.

13. Basel Committee on Banking Supervision. "Principles for Operational Resilience." The Bank for International Settlements. The Bank for International Settlements, August 6, 2020.

14. Federal Financial Institutions Examination Council (FFIEC). "Information Technology Examination Handbook." Federal Financial Institutions Examination Council (FFIEC), November, 2015.

15. Federal Financial Institutions Examination Council (FFIEC). "Information Technology Examination Handbook." Federal Financial Institutions Examination Council (FFIEC), November, 2015.

16. The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. "Sound Practices to Strengthen Operational Resilience." The Federal Reserve, November 2, 2020.

17. Computer Security Resource Center. "Glossary." National Institute of Standard and Technology.,csrc.nist.gov/glossary.

18. Computer Security Resource Center. "Glossary." National Institute of Standard and Technology.,csrc.nist.gov/glossary.