Business Resilience Council

by Global Resilience Federation

# Operational Resilience Framework

# Rules – Version 2.0

ORF

***October 2023***

*This document has been designated as **TLP CLEAR** and may be distributed in whole without restriction, subject to copyright controls.*

**Key Contributors**

Special thanks to the volunteer team of industry professionals and subject matter experts who have contributed significant time and energy to the Business Resilience Council (BRC) task force to develop the Operational Resilience Framework (ORF).

ORF Chairman

- Trey Maust, Executive Chair, Lewis & Clark Bancorp, former CEO of Sheltered Harbor

BRC Chairman

- David LaFalce, SVP and Global Head of Operational Resilience, Wells Fargo

ORF Task Force

- Bob Blakley, Operating Partner, Team8
- Charles Blauner, Operating Partner, Team8
- Jennifer Buckner, SVP Technology Risk Management, Mastercard
- John Carlson, VP Cybersecurity Resilience, American Bankers Association
- Simon Chard, Managing Director, S&P Global
- Judy Erbs, VP Technology Risk Management, Mastercard
- Gina Gavito, VP Global Crisis Management, Capital Group
- Michael Herd, SVP ACH Network Administration, NACHA
- Susan Rogers, Executive Director Operational Resilience, SMBC
- Cari Parrish, VP BCM, Capital Group
- Ben Shariati, Assistant Director, UMBC Graduate Cybersecurity Program
- Alex Sharpe, Sharpe Management Consulting
- Dr. Georgianna Shea, Chief Technologist, Foundation for Defense of Democracies
- Spruille Braden, Global Head of Enterprise Resilience Planning, Citi
- Eustathios Triantafellou, Director KY3P, S&P Global
- Jon Washburn, Chief Information Security Officer, Stoel Rives LLP
- Sounil Yu, CISO and Author, Cyber Defense Matrix
- Jenifer Zurfluh, SVP Enterprise Risk Management, Incredible Bank

GRF Staff

- Bill Nelson, Chairman, GRF
- Mark Orsi, CEO, GRF
- Chris Denning, Director, Business Resilience Council
- Brian Katula, Technical Project Manager, GRF

We also want to thank all those that have reviewed the ORF, bringing your expertise to this industry driven effort. A dynamic and growing list of reviewers and supporters may be found on our website at https://www.grf.org/orf.

NOTE: Views and opinions expressed by ORF contributors and reviewers are their own and do not necessarily reflect those of their affiliated organization.

# Contents

This Documentation is provided on an "AS IS" basis, without warranty of any kind. Global Resilience Federation disclaims all warranties with regard to this documentation, including all implied warranties of suitability and fitness for any particular purpose. In no event shall the Global Resilience Federation be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of this documentation.

Business Resilience Council

by Global Resilience Federation

## About Us

Global Resilience Federation (GRF) is a non-profit which manages and supports seventeen different information sharing and analysis organizations. GRF's mission is to help assure the resilience of critical and essential infrastructure against threats that could significantly impact the orderly functioning of the global economy and general safety of the public.

GRF formed the Business Resilience Council (BRC) in 2021 as a member-driven, multi-sector community created to build sharing and cooperation regarding significant incidents, threats and vulnerabilities that impact business operations. There are four pillars to the BRC mission:

1) Providing members with sharing of threats, incidents, vulnerabilities, and resilience best practices across cybersecurity, physical, and geopolitical concerns.
2) Fostering a collaborative, collective defense community including vendors, partners and suppliers to address third-party and supply chain risk.
3) Providing a framework and best practices for operational resilience in response to destructive attacks.
4) Organizing and leading cross-sector exercises simulating real-world threats and challenges.

The BRC initiated the Operational Resilience Framework (ORF) effort and working group in March 2021 with support from several large enterprises and government agencies. The vision of the ORF is to reduce operational risk, minimize service disruptions and limit systemic impact from destructive attacks and adverse events.

# Foreword

By David LaFalce, SVP and Global Head of Operational Resilience, Wells Fargo
Trey Maust, Executive Chair, Lewis & Clark Bancorp, former CEO of Sheltered Harbor

## What Is Resilience?

What does it mean to be resilient? At the top level, enterprise resilience, is the ability and capacity to withstand systemic shocks and adapt to emerging risks. At an aggregate level a resilient organization effectively aligns its strategy, operations, management systems, governance structure, and decision-support capabilities so that it can uncover and adjust to continually changing risks, endure disruptions to its primary earnings drivers, and create advantages over less adaptive competitors[1], while understanding its role in the broader ecosystem. This capability allows the organization to have the capacity to anticipate and react to change, not only to survive but to evolve.[2] In order to ensure there is enterprise resilience sub-disciplines need to be resilient. Typically, these include financial, technology, business, and operational. As a note, in some frameworks financial resilience falls under the operational resilience umbrella.

## What Is Operational Resilience?

Gartner defines operational resilience as initiatives that expand business continuity management programs to focus on the impacts, connected risk appetite and tolerance levels for disruption of product or service delivery to internal and external stakeholders (such as employees, customers, citizens and partners). These initiatives coordinate management of risk assessments, risk monitoring and execution of controls that impact workforce, processes, facilities, technology (IT, OT, IoT, physical and cyber-physical) and third parties across the following risk domains used in the business delivery and value realization process:

- Security (cyber and physical)
- Safety
- Privacy
- Continuity of operations
- Reliability[3]

A simple definition is a business's ability to respond to and overcome adverse circumstances during operation that might cause financial loss or disrupt business services;[4] this may mean running in an impaired state.

Operational resilience is not a new concept. In fact, the financial sector has been keenly focused on ways organizations can prepare for and respond to potentially disruptive events for decades. Resilience is the newest "R word" out there. First there was recovery (which is essential for business continuity and technology partners); then there was resumption; and now, resilience. Each iteration has matured to encompass and integrate more strategic considerations, moving from being simply a set of actions to representing a new mindset. However, with the financial services ecosystem and external threats continuing to evolve, firms are taking a fresh look at how they can further improve their operational resilience.

Operational resilience is an area of growing focus across the global markets. Today, companies face more threats than ever before. Social and political unrest continues, climate change is causing unprecedented challenges, cybersecurity threats are growing, and Covid-19 highlighted the fragility of supply chains and organizational design. In this increasingly complex environment, firms must be resilient and able to adapt their operations and processes to function under disruptive conditions while ensuring their ability to provide critical services.

If business continuity is the immediate plan to ensure that a business is able to continue providing services and survive, then operational resilience is the larger strategy that business continuity supports. Just about every organization has a business continuity plan, and if they didn't before 2020, they certainly have one now. While business continuity plans serve as an important backstop in the event of an unplanned incident or emergency, it is actually just the beginning of a set of best practices that ultimately lead to operational resilience.

### Looking Beyond the Organization

While business continuity focuses exclusively on the firm or more granularly products and supporting functions, its evolution to resilience means that it is equally concerned with internal factors as with external influences. A resilient firm is, in fact, especially cognizant of its role in its industry ecosystem, and understands the spillover effects that one organization can have on another.

The broader industry ecosystem has its own interconnections and dependencies, and it must be looked at holistically. It's important to consider not only employees and customers, but also vendors, regulators, industry associations, and other partners. Furthermore, in the same way that some processes are more critical to resilience than others, some external relationships, such as those with regulators, are especially important, as they can have a significant impact on the firm.

### Transcending Discrete Disciplines

One impedance that is immediately apparent is the commonly held view that operational resilience is a discrete discipline on the same layer as functions like business continuity, third party risk management and global security. All of these are actually part of the broader umbrella that is operational resilience. Maintaining their separation does not allow for control integration against common threats.

First, rather than narrowly focusing on systems, resilience-enhancing practices should aim to safeguard critical business services against a wide range of technical and physical disruptions. It exists as a holistic and strategic framework that is embedded across an entire organization. This supports a better integration of functions, the use of proper operational maps, and the effective management of both internal and external factors. Examining business processes through such a comprehensive lens is essential for firms looking to shift from continuity to ongoing resilience, which will allow them to better adapt - and continuously evolve - in the face of external change.

Second, industry coordination and cooperation will be a key measure of success. The very nature of systemic risk requires a collaborative process and coordinated effort, within companies and across industries, to help detect systemic shocks before they strike and to recover from them as quickly as possible. Ongoing sector-wide collaboration and testing will be necessary to ensure all firms understand their roles and have the appropriate level of readiness to mitigate factors that could disrupt their critical business services.

Third, firms must strive to promote a “resilience-centric” corporate culture, fostering a mindset that focuses on continuous improvement when it comes to resilience that is supported by the firm’s board and senior management. Employees should be encouraged to challenge the status quo and create a mindset that is based on continuous learning. The ever-growing risks to the industry are far too great, and we must continue to evolve our resilience practices and capabilities to meet the demands of tomorrow while continuing to safeguard the markets today.

## Adopting a Maturity Model

In order to organize internal and external factors within a resilience framework, organizations can utilize maturity models that incorporate a number of measurements covering factors including planning, people, governance, technology, reaction, and reporting. They can also look at resilience on different levels, from product, to legal entity, to enterprise. This becomes a visual representation of resilience for the firm, cutting across levels and factors.

# Executive Summary

Operational resilience is the ability to reliably provide critical services in the face of any disruption. The Operational Resilience Framework (ORF) was made public in 2022. In the year since the initial release, the Business Resilience Council's task force has expanded the framework to include a maturity model and several worked examples. Additionally, the team has worked to incorporate ORF principles and rules into significant efforts such as the President's Council of Advisors on Science and Technology (PCAST) working group on cyber-physical resilience, and The National Automated Clearing House Association's white paper, "Enhancing Operational Resilience for ACH Network Participants."

The ORF builds upon many earlier works on Operational Resilience such as the July 2018 Bank of England discussion paper, "Building the UK financial sector's operational resilience," and other publications from regulatory bodies, trade association alliances, and individual institutions who have launched various coordinated efforts to define expectations and develop an approach to operational resilience. However, these remain in the exploration and taxonomy phase, with firms continuing to focus on traditional disaster recovery and business continuity efforts. These approaches have been insufficient in the past, especially in the face of destructive events such as ransomware, wiperware, and data center fires.

Recently, we have witnessed devastating losses stemming from deficiencies in Operational Resilience. These stark examples include Lincoln College, an HBCU, which was forced to halt its operations after 157 years due to a ransomware attack. St. Margaret's Health had to permanently close its hospitals, clinics and other facilities. At the time of writing, MGM anticipates a substantial blow, with expected quarterly profit losses of at least $100 million, while Clorox foresees an impact on sales of over $500 million from due to cyberattacks. These incidents underscore that even organizations with robust disaster recovery plans in place remain vulnerable to disruptions that may be catastrophic.

In 2021, the Global Resilience Federation's Business Resilience Council (BRC) initiated the effort to develop the Operational Resilience Framework (ORF) rules with support from subject matter experts and professionals across several industries. The BRC is an all-hazards information sharing organization that operates across all sectors to build strong collaborative communities and regional efforts that create stability in times of crisis. In 2023, the BRC began to develop version 2.0 of the ORF, with a strong focus on building a maturity model and some minor updates to the rules.

The goal of the ORF working group is to develop and refine a framework of rules and tools to benefit organizations of all sizes. These rules provide continuity and recovery of critical data, systems and processes required to minimize service disruptions to customers, partners and counterparties minimizing systemic damage and limiting cascading disruptions. Together they enhance the operational continuity of vital infrastructure, individual organizations, industries and sectors in the face of adverse events and destructive attacks.

Key features of this initiative include (i) planning for delivery of operations critical services in an impaired state to predefined groups of customers, partners and counterparties until services can be fully restored; (ii) implementing distributed, immutable backup and restoration systems for the user and business data, systems, applications, networks, and configurations supporting operations critical services; and (iii) requiring executive-level sponsorship and support from the business to build a culture of operational resilience that achieves resilient business services.

This initial set of rules was reviewed by hundreds of companies and regulatory bodies, and we have worked to incorporate feedback in all of the ORF documents. The rules have been aligned with existing control frameworks from the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and others, and are expected to be refined and improved annually to become the definitive standard for Operational Resilience.

I extend my heartfelt gratitude to David LaFalce, Chair of the BRC, and Trey Maust, Chair of the ORF, as well as our unwavering task force members and all those who have made invaluable contributions to this endeavor thus far. Your dedication and commitment are truly commendable.

As you review and test this framework in your organization, please add your voice to this initiative to help us improve the rules and job aids, making this even more useful and accessible. Reach out to us at orf@grf.org for more information or to get involved. With support from hundreds of GRF affiliated companies and implementers like you, we will continue our efforts to develop exercises and aids to educate boardrooms, executives, and resilience professionals on how to strengthen their operational resilience.

Mark Orsi
CEO, Global Resilience Federation

# Introduction

In 2014, Sony Pictures was attacked with wiperware called Destover, similar to the Shamoon malware used on Saudi Aramco in 2012. This devastating attack erased data on hundreds of servers and thousands of systems. In the face of these types of destructive attacks and the risk that they posed to the financial sector, several US banks worked together on an initiative called Sheltered Harbor to safeguard essential consumer data by generating immutable backups in a standard format. If a bank's systems were erased or destroyed, the data could be recovered – protecting consumer and public confidence in the banking system irrespective of the nature and severity of the hazard that caused the outage.

In 2018, the Bank of England released a seminal paper titled "*Building the UK financial sector's operational resilience*" emphasizing the critical role of Operational Resilience in the banking sector to avert systemic disruptions. The guidance emphasized the need for operational resilience including continuity of important business services, definition of tolerable disruption levels, and construction of resilient services assuming disruptions will occur. In 2020, the United States Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation jointly issued an interagency paper in 2020 titled "Sound Practices to Strengthen Operational Resilience." This has brought renewed focus, particularly concerning critical services provided by businesses to customers, partners and counterparties.

Today, Sheltered Harbor is widely adopted in the US financial sector to safeguard a limited set of consumer data, but this is incomplete. The need goes further, to include enabling critical services in the face of significant disruptions across various sectors, even if they must operate in a compromised state. The focus should not solely be on recovering business and consumer data, but also restoring the systems, networks, applications and configurations essential for rapidly resuming important business services, thus preventing further systemic impacts and harm to the broader ecosystem.

In 2021, Global Resilience Federation embarked on the mission to develop and refine the Operational Resilience Framework (ORF) rules with the support of subject matter experts and professionals spanning multiple industries. The mission statement for this activity is:

**ORF Mission Statement:**
To develop and refine an industry-driven framework of rules which provide continuity and recovery of critical data, systems and processes required to minimize service disruptions to customers, business partners and other counterparties; enhancing the operational continuity of vital infrastructure, individual organizations, industries and sectors in the face of adverse events and destructive attacks.

The ORF aims to provide a set of rules that minimize service disruptions and enhance operational continuity. Utilizing the ORF and its accompanying Maturity Model, organizations can:

- Gain a comprehensive understanding of their Business Critical and Operations Critical services
- Map out the systems and processes supporting these services
- Develop resilient systems that deliver Operations Critical services in predesigned impaired states during a crisis
- Effectively test resilience plans both internally and with external stakeholders

Additionally, the ORF Maturity Model serves as a vital tool for organizations to assess their progress and readiness in implementing operational resilience practices. The ORF aligns with established standards like NIST, ISO and ITIL, offering a flexible yet robust framework for organizations of all sizes. The goal is to weave resilience into our interconnected ecosystem and to continuously refine the framework based upon feedback and evolving needs from industry.

## Path to Operational Resilience

Designed for executives, risk management professionals, and practitioners of operational resilience in both business-aligned and technology-aligned roles, this section provides a structured pathway to operational resilience. Consisting of seven key steps rooted in foundational principles of risk management, cybersecurity, and information technology, this guide aims to be both adaptable and rigorous. You are encouraged to consider these steps in the context of your organization's unique operational needs, constructing a resilience plan that not only withstands adverse events but also enhances operational continuity to serve your customers, partners, and the broader ecosystem.

In some cases, an organization may continue progress toward operational resilience with incomplete information, and refine over time, learning from each iteration. We leave the details up to the implementer and welcome feedback that may help others through the process. The steps are captured in the following table and described below:

### Path to Operational Resilience

1. Implement industry-recognized risk management, information technology and cybersecurity control frameworks.
2. Understand the organization’s role in the ecosystem.
3. Define the Minimum Viable Service Levels for each Operations Critical and Business Critical service.
4. Establish Service Delivery Objectives for each Operations Critical and Business Critical service.
5. Preserve the Data Sets necessary to support Operations Critical and Business Critical services.
6. Implement processes to enable recovery and restoration of Operations Critical and Business Critical services to meet Service Delivery Objectives.
7. Independently evaluate design and test periodically.

The detailed ORF Rules can be found in Appendix-1. Additional documentation including a glossary, tools, and illustrative examples can be found at https://www.grf.org/orf.  Each of the seven steps are described below, followed by discussion on how the ORF differs from traditional Business Continuity Management (BCM).

### Step 1 – Build the Foundation

First on the path for any organization is to implement industry-recognized IT and Cybersecurity control frameworks like NIST 800-171, NIST 800-34, ISO 27001, ISO 22301 and ITIL. This is a foundational step in development of Operational Resilience as many of the rules within the ORF were written with the expectation that the organization has an understanding and commitment to risk management through implementation of standardized controls. In addition to implementing industry-recognized controls, this step requires executive sponsorship and assurance that the ORF recommended policies, procedures and mechanisms will be resourced appropriately to sustain them through organizational, internal and external changes.

Goals for this step are to establish a robust governance structure for operational resilience aligned with industry best practices, led by a qualified executive and designed to be sustainable through organizational changes. Main points include:

- An implemented and documented set of industry standard controls
- A newly defined organizational role
- Budget
- Program documentation

### Step 2 – Understand the Ecosystem

The second step on the path is to understand the organization's role in the ecosystem. This requires the inventory and prioritization of outward-facing services and entities that consume the services. An important concept in this step is determining the criticality of services by categorizing them as Operations Critical, Business Critical or All Other. Those outward-facing services that require near-continuous functioning to limit service disruptions and impacts to customer are designated as Operations Critical. Services that are required for the organization's business continuity and don't meet the Operations Critical criteria are designated as Business Critical.

The expected outcomes for Step 2 focus on gaining a comprehensive understanding of the organization's role in the broader ecosystem, specifically in terms of service delivery and its impact on various stakeholders. Main points include:

- A comprehensive documentation of services and dependencies
- Categorization of services
- Prioritized customer and partner groups

### Step 3 – Define Minimum Viable Service Levels

The third step is to define the Minimum Viable Service Levels for each critical service. To do this, the organization must identify the internal processes which support service delivery. Then a high-level analysis of potential failure modes is performed to identify the types of service disruptions that may occur regardless of the root cause. The organization must then consider the demands for each customer, partner and counterparty group to define the Minimum Viable Service Levels that are still usable and valuable to each defined group. This is directly related to the Bank of England's term "Impact Tolerance" as follows: a disruption to an important business service that exceeds the defined Impact Tolerance results in an impaired service below the Minimum Viable Service Level.

Step 3 expected outcomes revolve around setting the groundwork for service resilience by detailing the Minimum Viable Service Levels. The aim is to dissect services, understand their building blocks, potential points of failure, and minimum levels at which they can operate without causing significant harm or disruption. Achieving these main points informs later steps, planning and response strategies:

- Detailed mapping of service dependencies and failure mode analysis
- Minimum Viable Service Levels for each critical service and prioritized customer group, understood and agreed upon by stakeholders

### Step 4 – Establish Service Delivery Objectives

The fourth step is to establish Service Delivery Objectives for each critical service. This requires a detailed analysis of the design of each service including the internal and external dependencies across people, process, technology, vendors, and suppliers. Up to this point, the ORF process has been primarily business driven – with focus on outcomes to customers and partners. In step four, technology teams must be engaged to ensure the Service Delivery Objectives are achievable and to help establish the Target Operational Service Levels. This is a reduced set of target service levels with considerations of Minimum Viable Service Levels required by the various customer groups. These target service levels are then analyzed and expanded to detail the technical Service Delivery Objectives for the components used to deliver each critical service.

For Step 4, the expected outcomes establish detailed service and data restoration objectives, including the mechanics of how services will be delivered under varying conditions and how data will be restored – both crucial for operational resilience. Organizations will be setting groundwork for plans to maintain service delivery and data availability under adverse conditions. Main points include:

- Target Operational Service Levels
- Service Delivery Objectives
- Data Restoration Objectives
- Documentation and process updates to incident management and communications plans
- New and updated third-party agreements

**Example – Acme Company**

As a simplified example of the third and fourth steps, consider Acme Company with an Operations Critical service to process transactions for three customer groups. After an analysis of their service capacity, Acme Company determines it typically processes 20K transactions per hour during normal operations. Acme Company has contractual obligations to process 4K transactions per hour for Group A, 5K transactions per hour for Group B, and 6K transactions per hour for Group C, with a grand total of 15K transactions per hour across all three customer groups. Through estimation, Acme Company believes if it were in a crisis situation, Groups A, B, and C would be able to continue their operations if Acme Company can process at least 3K transactions per hour for each group while working to restore full throughput. This establishes the Minimum Viable Service Levels for the customer groups.

In this case, Acme Company decides to develop redundant systems and contract with alternate services providers to meet three Target Operational Service Levels – 15K transactions per hour (full contract delivery to all three Customer Groups), 9K transactions per hour (Minimum Viable Service to all three Groups or full service to Groups A and B), and 6K transactions per hour (no service to one Group, impaired service to two Groups). Detailed Service Delivery Objectives are then produced as input to the fifth and sixth steps.

### Step 5 – Preserve Critical Data Sets

The fifth step is to preserve the data sets required for critical services including considerations for confidentiality, integrity, and availability. Data Restoration Objectives are defined to enable recovery within the constraints set by the Service Delivery Objectives. A key distinction made by the ORF from other control standards is the definition of Critical Data Sets which must be immutably backed up to enable recovery. The Critical Data Sets must include not only consumer and business data, but the applications, systems, networks, core infrastructure services, and configurations required to restore the services, even if in an impaired state. There have been many cases where core infrastructure services such as Active Directory were unavailable, leading to significant service outages in large enterprises. By ensuring backups of these additional data set components, these outages can be minimized.

Step 5 is focused on data availability and integrity even in adverse conditions. This step preserves data to meet the objectives set in Step 4. This involves a comprehensive approach to managing the format, frequency, confidentiality, integrity and availability of Critical Data Sets. Expected outcomes involve creating robust processes and mechanisms to secure, validate and manage Critical Data Sets:

- Critical Data Set format and frequency
- Confidentiality, integrity and availability of Critical Data Sets
- Data permanency, retention and deletion

### Step 6 – Enable Recovery

The sixth step is to implement systems and processes to enable recovery and restoration of critical services to meet the Service Delivery Objectives. This includes establishing a recovery environment and implementing systems and processes sufficient to achieve the Service Delivery Objectives. Other important aspects of this step are to ensure redundancy for authorized access to archives and ensuring cryptographic keys are available for restoration processes. Documentation including Incident Response Plans, Recovery Plans, and both internal and external Communications Plans must be updated.

This step enables robust recovery mechanisms that align with previously defined objectives. The emphasis is on automating recovery processes, ensuring redundancy in archive access, and updating incident, recovery and communications plans. Expected outcomes include:

- Recovery Environment and data restoration mechanisms
- Cryptographic protections and access redundancy
- Updated incident, recovery and communications plans

### Step 7 – Independently Test

And the last step is to Independently evaluate the design and periodically test the organization’s implementation of the Operational Resilience Framework and its ability to meet Service Delivery Objectives and associated business outcomes. This includes testing by a team independent of the implementation team and updating the implementation to meet any changes to the sector, organization, business model, information systems, or the environment of operation.

Step 7 is focused on ongoing verification, validation and improvement of operational resilience measures. The expected outcomes include:

- Independent evaluation of architecture, design and policies
- Independent testing to ensure alignment with Service Delivery Objectives
- Monitoring for coverage and effectiveness

- Continuous improvement and problem resolution

### Difference from Traditional Business Continuity

Through these seven steps, an organization can build, manage, and continuously improve their Operational Resilience. The rules were designed alongside each of these steps. The ORF rules can be found in Appendix 1 - Rules.

The ORF approach builds upon traditional Business Continuity Management (BCM) activities in several ways. BCM focuses on full recovery of business systems in response to specific scenarios by using well formulated tools to support crisis management, business continuity planning, and IT disaster recovery. The Operational Resilience Framework (ORF) extends this model with a more holistic approach to include the needs of prioritized customer, business partner, and counterparty groups, and designing impaired states of service operation to prevent systemic issues and significant impacts to the ecosystem. ORF is business driven, addressing resilience at the external service level across the people, process and technology required to drive the service. There is a much stronger business lens on the ORF activities than in traditional, IT-led BCM.

The ORF builds upon these concepts to design operations critical services that support intermediate, impaired operational states while the organization works in parallel to achieve full recovery. To achieve this, Operations Critical Services may require new technologies, business processes, additional resources, and additional contractual agreements with vendors and suppliers. The ORF rules also extend the legacy definition of critical data sets from business and customer data to include the data required to configure and run the applications, networks, systems and processes that support critical services. All data supporting operations critical services must be backed up in a distributed and effectively immutable way to ensure critical services can be quickly restored to a target impaired service level during a crisis. The advent of distributed and effectively immutable storage from cloud service providers makes this type of backup widely accessible and available to most organizations.

## Key Terms

The ORF was designed to minimize the introduction of new terms, and to re-use language from existing standards organizations wherever possible. When progressing the state of the art, it is often necessary to craft new terminology to cement concepts and to foster communication. The full glossary is included in the *ORF_v2_Glossary* document but the following lists a few new terms that represent important concepts required to describe Operational Resilience, building on earlier works.

**Operational Resilience Executive** – The qualified executive with the responsibility and authority to ensure appropriate organizational support, implementation, and oversight for Operational Resilience.

**Customers, Partners and Counterparties –** The entities that would be impacted by disruptions to an organization's products or services. Customers are entities and individuals that consume an organization's products or services. Partners are entities which have contract or agreement with an organization. Counterparties include entities which have an obligation, contract, or agreement associated with an organization's products or services. All three of these groups would be impacted by disruption of an organization's products or services.

**Minimum Viable Service Level** – The lowest possible level of service delivery (i) to enable customers, partners and counterparties to continue their operations without significant disruption to the delivery of their critical services to their own customers, partners and counterparties; or (ii) if the customer is an individual, to minimize consumer harm.

**Operations Critical Service** – A service provided by the organization that requires near continuous functioning, even if at impaired levels, to limit disruptions and impacts to customers, partners and counterparties.

**Business Critical Service** – A service that is required to prevent sustained disruption to the organization's continuity and ability to deliver services to customers, partners and counterparties.

**All Other Services** – The services necessary to support the business at pre-event levels that cannot be categorized as Operations Critical or Business Critical.

**Operations Critical and Business Critical Data Sets** – Comprehensive data sets supporting recovery and restoration of critical services including user data, business data, processes, applications, networks, systems, core services and configurations.

**Service Delivery Objectives** – The objectives that set the impaired level and time constraints for delivery of Critical Services in the event of a disruption.

**Data Restoration Objectives** – The objectives that define the specific data sets that must be restored to reach the impaired level of operationality set by the Service Delivery Objectives.

**Operational Resilience Plan** - The plan used to guide an enterprise-wide response to an adverse event or destructive attack which ensures continuity of critical services to meet Service Delivery Objectives.

# ORF Maturity Model

The ORF Maturity Model is an integral component of Version 2.0 of the Operational Resilience Framework. This model offers organizations a methodical, step-by-step approach for bolstering operational resilience against an ever-changing landscape of disruptive threats.

## Core Structure

The model provides the tools to evaluate an organization's operational resilience across two distinct dimensions: Implementation Maturity and Assessment Maturity. By making this distinction, organizations can provide more comprehensive and nuanced information to stakeholders. Each dimension is characterized by five stages, allowing organizations to methodically progress from initial design to ongoing refinement for each rule and step in the framework. First, we describe the Implementation Maturity levels:

### Implementation Maturity Levels

- **L0 - Unspecified:** Initial stage where no specific processes or mechanisms have been designed for a given rule.
- **L1 - Designed:** Processes and mechanisms have been designed but are not fully implemented.
- **L2 - Implemented:** Processes and mechanisms are implemented, potentially in a pilot phase, but not fully operational.
- **L3 - Operating:** Processes and mechanisms are fully operational, but continuous refinement is yet to be attained.
- **L4 - Refining:** The apex of maturity, featuring a comprehensive array of resources, metrics, governance, and continuous improvement mechanisms for each rule.

Assessments typically begin when an organization approaches or reaches an implementation maturity of Level 3 – Operating. To reach full maturity, the robust implementation must also be validated independently for both completeness and performance. The Assessment Maturity Levels are:

### Assessment Maturity Levels

- **A0 - Not Assessed:** No assessment has been conducted.
- **A1 - Internal:** An internal assessment, typically by compliance or audit teams.
- **A2 - Independent:** An unbiased assessment conducted either internally or externally.
- **A3 - Completeness Audit:** A comprehensive audit focused on the completeness of the rule's implementation.
- **A4 - Performance Audit:** A rigorous audit evaluating the effectiveness of the rule in contributing to operational resilience.

## Documentation and Validation

As organizations progress through the implementation maturity levels, the documentation requirements escalate, ranging from initial design documents to comprehensive management plans. These documents serve both as a roadmap for internal teams and as validation artifacts for assessments.

## Maturity Level Example

This example will illustrate the maturity model and suggested implementation artifacts for one of the rules in the ORF. In this scenario, we extend the example of Acme Company on page 10, focusing on how Acme Company approaches Rule 4.1, which deals with establishing Target Operational Service Levels in alignment with Minimum Viable Service Levels for their customer groups.

### Scenario: ACME Company's Transaction Processing Service

Acme Company provides an Operations Critical service that processes transactions for three distinct customer groups: A, B and C. They have obligations to process 15K transactions per hour across all groups and have set Minimum Viable Service Levels at 3K transactions per hour for each group during crisis situations. The company's Internal Audit team, supported by the Operational Resilience Executive (ORE) conducted an assessment of Acme's Operational current operational resilience state.

### Implementation Maturity Levels for Rule 4.1 – Delivery Objectives: Service Design

Rule 4.1 mandates the establishment of Target Operational Service Levels, considering the Minimum Viable Service Levels required by customers and the service dependencies. The ORF_v2_Maturity_Model spreadsheet, "ORFv2 Rules" worksheet provided the following guidance for Implementation Levels L1 to L4 as follows:

- Level 1 – Designed: Organization has designed the processes and mechanisms to establish and document Target Operational Service Levels for each Operations Critical and Business Critical service.
- Level 2 – Implemented: Organization has implemented the processes and mechanisms to establish and document Target Operational Service Levels for each Operations Critical and Business Critical service.
- Level 3 – Operating: Organization has establishing and documenting Target Operational Service Levels for each Operations Critical and Business Critical service.
- Level 4 – Refining: Organization updates, reviews and ratifies documented Target Operational Service Levels for each Operations Critical and Business Critical service upon change to the services and at a defined cadence. Organization measures, monitors and manages associated processes to achieve better accuracy and completeness.

Further, the worksheet indicated Suggested Implementation Artifacts as follows:

- Program documentation
- RACI, role description, organizational chart
- Process for establishing and refining Target Operational Service Levels
- Documented Target Operational Service Levels
- Evidence of compliance review by internal/external counsel
- Documentation of changes, reviews and ratification

During implementation, the Operational Resilience Executive ensured her teams followed guidance for the suggested documentation.

As described earlier, the company can typically process 20K transactions per hour (tph) and has contractual obligations to provide at least 15K tph across customer groups A, B and C. Through estimation, Acme believes groups A, B and C would be able to continue their operations if Acme can process at least 3K tph per group. Acme further prioritized the groups and created the following tables for Target Operational Service Levels:

| Cusomer Group | Group Priority | Standard SLA | Minium Viable Service Level | Target Crisis Level 1 | Target Crisis Level 2 |
|---|---|---|---|---|---|
| A | High | 4K | 3K | 3K | 3K |
| B | High | 5K | 3K | 3K | 3K |
| C | Medium | 6K | 3K | 3K | 0K |
| | Totals | **15K** | **9K** | **9K** | **6K** |

all quantities in the table are transactions per hour

During implementation of ORF Rules, Acme's Operational Resilience Executive worked with the engineering team to develop redundant systems and entered into contracts with alternate service providers. Acme then defined three Target Operational Service Levels:

- Standard SLA – 15K transactions per hour providing full contract delivery
- Crisis Level 1 – 9K transactions per hour providing the minimum viable service to all three customer groups
- Crisis Level 2 – 6K transactions per hour providing the minimum viable service to highest priority customer groups.

These levels were tested using the redundant systems and alternate service providers. After Acme's teams gathered evidence and performed an internal review against the ORF Maturity Model, they concluded Acme had reached an implementation maturity level of **L3: Level 3 – Implemented** and an assessment maturity level of **A1: Level 1 - Internal** for rule 4.1.

## Implementation Aids

There is additional work to be done to support implementation of the Operational Resilience Framework. The table below indicates the types of templates and implementation aids that will be made available, organized by the steps in the ORF Path to Operational Resilience. The development effort for these aids is ongoing. Links to these tools will be added to the website as they become available at https://www.grf.org/orf.

| Step | Path Step Description | Implementation Aid |
|---|---|---|
| 1 | **Implement industry-recognized risk management, information technology and cybersecurity control frameworks.** | Self-assessment, primer and required supports for the Operational Resilience Executive to initiate the program. |
| 2 | **Understand the organization's role in the ecosystem.** | Guide and examples for enumeration, grouping and prioritization of customers, partners and counterparties and the identification of dependencies. |
| 3 | **Define the Minimum Viable Service Levels for each Operations Critical and Business Critical service.** | Guide with mechanisms and examples to help define the Minimum Viable Service Levels. |
| 4 | **Establish Service Delivery Objectives for each Operations Critical and Business Critical service.** | Mechanism and examples to support definition of Service Delivery Objectives for Critical Services for each customer, partner and counterparty. |
| 5 | **Preserve the Data Sets necessary to support Operations Critical and Business Critical services.** | Reference Architecture to provide architecture and design examples currently achievable with given tools and technologies. |
| 6 | **Implement processes to enable recovery and restoration of Operations Critical and Business Critical services to meet Service Delivery Objectives.** | Operational Resilience Plan templates to guide an enterprise-wide response to an adverse event or destructive attack to ensure continuity of critical services within pre-defined Service Delivery Objectives. |
| 7 | **Independently evaluate design and test periodically.** | Assessment tool and guidance for independent testing, monitoring, and continuous improvement. Implementation of control instrumentation, measurement, and monitoring. |

## Future Activities

With the ongoing backing of stakeholders from industry, government, and regulatory organizations, as well as the invaluable input from the Global Resilience Federation's Business Resilience Council, we are committed to the regular review and timely updates of the Operational Resilience Framework (ORF) rules. This process will be conducted annually or more frequently as needed. In addition, we are actively developing practical aids and tools for ORF implementation, all of which will undergo periodic review and updates to ensure their continued relevance and utility. Our aim is to produce resources that facilitate the adoption and execution of the ORF across organizations, regardless of their size or sector.

We invite you to become an integral part of these initiatives. To lend your expertise to our working groups, please contact us directly at orf@grf.org. For those interested in a deeper level of involvement and additional benefits, membership in the Business Resilience Council offers a unique opportunity to participate in an all-hazards, multi-sector collective defense community. This includes access to a diverse network of vendors and suppliers, all united in the common goal of enhancing resilience.

If you'd like to join the growing number of professionals who are reviewing and supporting the ORF, you can add your name via the form available at https://www.grf.org/orf. All submissions will be kept anonymous unless you specify otherwise. Your participation and feedback are not just welcomed; they're essential for the continual improvement and success of the ORF. Thank you for considering how you can contribute.

**Implementation Aid Development:** This is an ongoing effort to develop templates and job aids to support the Operational Resilience Executive and the ORF implementation team within the organization through the steps to achieve operational resilience. The development effort for these aids is ongoing with expectation for them to be released with the final draft of the ORF Rules.

**Scenarios and Exercises:** The ORF working group continues to develop interactive scenarios and exercises. These will be developed to show the approaches and resources that contribute to the implementation of the ORF, with an emphasis with how it strengthens the organization. There will be a wide range of these exercises and scenarios so that organization of all sizes and shapes can relate to them and learn from them. Current examples available at https://www.grf.org/orf include:

- ACME Pipeline – a business-oriented scenario based upon a petroleum pipeline very similar to Colonial Pipeline.
- ACME Financial Services – a mid-sized financial institution that originates and receives electronic payments and money transfers using the Automated Clearing House (ACH) network.

**Operations Technology Expansion:** With support from the newly launched Manufacturing ISAC, a working group will be established to expand the ORF Rules to address the concerns regarding Operational Technology (OT) Systems, Industrial Control Systems (ICS), and the Internet of Things (IoT).

**Review of Materials and Continuous Improvement:** The ORF is meant to be a cross-industry framework to guide any organization in the development, deployment, and maintenance of operationally resilient services. Organizations are encouraged to submit ideas and commentary, join BRC working groups and make contributions to further this effort. If you have recommendations for tools, best practices, scenarios or other supports that will foster adoption and ease implementation of the ORF, please send them to orf@grf.org.

# Appendix 1 - Rules

The following are the Operational Resilience Framework Rules – Version 2.0. A spreadsheet with more information including the ORF Maturity Model, a mapping to NIST and ISO controls, and change tracking from Version 1.0 can be found at https://www.grf.org/orf.

## Step 1 - Implement industry-recognized risk management, information technology and cybersecurity control frameworks.

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 1.1 | Governance: Security Controls | The organization must implement an industry-recognized information technology, risk management and cybersecurity control framework. | A foundational step in development of Operational Resilience is to establish primary information technology and security controls within an organization. Data must be protected and managed in accordance with company, statutory and regulatory requirements including privacy, security, data protection, data management, continuity of business and other policies, practices and procedures.<br>All changes to ORF policies, procedures, mechanisms and configurations must follow defined change control processes and requisite approvals. The Operational Resilience Framework assumes knowledge and prior implementation of standards-based control frameworks such as those from the National Institute of Standards and Technology (e.g.: NIST SP 800-53) and the International Organization for Standardization (e.g.: ISO 27001). See the glossary definitions for Cybersecurity Control Framework and Technology Control Framework for more examples. |
| 1.2 | Governance: Executive Sponsorship | The organization must designate a qualified executive as both responsible and accountable to ensure appropriate organizational support for operational resilience. | This rule establishes the Operational Resilience Executive (ORE) as a key role with ownership and accountability for implementation of Operational Resilience within the organization. This executive may have board-level visibility and broad reach across business, technology and risk functions with insight into products and services delivered to customers, partners and counterparties, as well as the people, processes, technology and dependencies required to deliver those services. The Operational Resilience Executive must work to build the culture of resilience in the firm required to achieve resilient business services.<br>NOTE: Organizations may not require a dedicated resource for this role. Larger, more mature, or complex organizations may consider a dedicated executive. |
| 1.3 | Governance: Sustainability | ORF policies, procedures and mechanisms must be documented, managed and resourced appropriately to ensure sustainability through organizational, internal and external changes. | Operational Resilience policies, procedures and mechanisms must be designed and implemented to be operationally effective and to survive organizational, internal and external changes. Related roles and responsibilities must be defined and assigned to staff or third-party services. |

## Step 2 – Understand the organization's role in the ecosystem.

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 2.1 | Ecosystem:<br>Service Catalog | The inventory of business services must be documented. | The inventory of external business services must be documented to ensure full coverage during the operational resilience implementation. At this stage, the core activity requires business executives to inventory the organization's services at a high level to enable further analyses.<br>Additional data collection should begin as supporting processes, systems, data sets and service dependencies must also be identified and documented prior to operational resilience implementation (Step 3.1). |
| 2.2 | Ecosystem:<br>Service Criticality | Business services must be designated as Operations Critical, Business Critical or All Other Services. | Operations Critical Services are external-facing and require near-continuous functioning to limit service disruptions and impacts to customers, partners and counterparties. Business Critical Services are required for the organization's continuity. This may include internal and back-office functions. Services that are not considered Operations Critical or Business Critical may be categorized as All Other Services. |
| 2.3 | Ecosystem:<br>Group Classification | Customers, partners and counterparties must be identified and grouped by common characteristics relevant to service delivery prioritization. | This step supports later prioritization efforts. Customers, partners and counterparties must be grouped and prioritized for each critical service. A template will be provided in the ORF toolkit. Grouping criteria may include services, contractual agreements, regulatory requirements, service level agreements, supply chain and other dependencies, potential sector impacts, size of the customer, revenue/income of the customer, income generated by services to the customer and other criteria relevant to prioritization efforts.<br>Where relevant, sector and cross-sector dependencies and potential impacts should be identified at global, national and regional levels for service delivery impairment. |
| 2.4 | Ecosystem:<br>Group Prioritization | A priority level for service delivery must be assigned to each defined customer, partner and counterparty group for each Operations Critical and Business Critical service. | Service delivery prioritization will enable development of informal service levels to deliver different levels of impaired services to defined customer, partner and counterparty groups up to and including full discontinuation of services. |

### Step 3 – Define the Minimum Viable Service Levels for each Operations Critical and Business Critical service.

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 3.1 | Minimum Viable Service:<br>Service Delivery | The supporting processes and both internal and external dependencies necessary for delivery of Operations Critical and Business Critical services must be identified. | Document how each critical service is delivered including people, processes, technologies, third-party, supply-chain and other dependencies.<br>In order to establish Operations Recovery Objectives, the organization must identify how each critical service is delivered and both the internal and external dependencies. The organization can then define its tolerance for impairment to internal business services and to upstream / supply chain services which support the critical services. Examples of dependencies:<br><br>**People:**<br>- Business Unit / Organizational Dependencies<br><br>**Process:**<br>- Payment Processing<br>- Line of Business Processes<br><br>**Technology:**<br>- Custom Hardware or Software<br>- Data Centers<br>- Cloud Providers<br>- Servers<br>- Applications<br>- Networks<br>- Configurations<br><br>**Third-Party:**<br>- Third-Party Service Providers<br>- Third-Party Equipment Providers<br>- Component / Materials Providers<br>- Ecosystem Sector and Cross-Sector dependencies<br>- Ecosystem Regional, National, Global dependencies<br>- Other Supply Chain dependencies<br><br>**Customers, Partners and Counterparties:**<br>- Customer, Partner and Counterparty agreements<br>- Readiness to receive service |

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 3.2 | Minimum Viable Service:<br>Failure Modes | Top-level failure modes and levels of impairment for each Operations Critical and Business Critical service must be identified. | A high-level analysis of services and potential failure modes must be performed to define the minimum service levels that can be delivered and that still satisfy the minimum requirements that can be tolerated by customers, partners and counterparties before the service is no longer useful.  This is a study of the types of service disruption regardless of the root cause. An example is a bridge with two of three lanes closed. It is not important to consider why the lanes are closed, only that the capacity of the bridge to process traffic may be 1/3 or less when the lanes are closed.<br>Failure modes may be determined through historical analysis of past service impairments, analysis of the service design, or other mechanisms. Critical failure scenarios that cause significant service disruptions should be included in the analysis, even if they are unlikely.<br>More mature organizations may perform iterative failure mode analysis once full internal and external dependencies are known for delivery of critical services. |
| 3.3 | Minimum Viable Service:<br>Minimum Service Levels | Minimum Viable Service Levels must be established for each customer, partner and counterparty group. | To better understand Minimum Viable Service Levels (MVSLs), the organization may perform customer surveys, testing and analysis to establish both formal and informal SLAs. The process includes estimating the service levels required for each critical service to customer, partner and counterparty groups and then identifying commonalities to reduce the set of service levels required.<br>The goal is to create a distinct set of minimum service levels for each prioritized group that provide the lowest possible level of service delivery (i) to enable defined groups of customers, partners and counterparties to continue their operations without significant disruption to the delivery of their critical services to their downstream customers, partners and counterparties; or (ii) if the customer is an individual, to minimize consumer harm.<br>It is important to note at this stage, the MVSL is established for each prioritized customer group, partner group and counterparty group. Target Service Levels are established later for operating in impaired states which may not meet MVSLs for all prioritized groups.<br>As the process matures, the organization may start formalizing the informal SLAs identified in development of MVSLs. |

## Step 4 – Establish Service Delivery Objectives for each Operations Critical and Business Critical service.

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 4.1 | Delivery Objectives: Service Design | Target Operational Service Levels must be established to include considerations of Minimum Viable Service Levels required by customers, partners and counterparties and identified service dependencies. | Service design may require updates to account for considerations of Minimum Viable Service Levels required by customers, partners and counterparties, identified service dependencies and key failure modes to include low probability but highly disruptive events. Options for impaired service delivery should be established and rationalized to create a set of target operational service levels. It is important to design the Target Operational Service Levels and transitions between these levels. This may require updates to incident management, communications plans and other existing processes.<br>Over time, work may be required to bolster mechanisms of service delivery across people, process and technology. This may be an iterative process to develop new options for impaired service delivery requiring significant changes such as: contractual updates or new service level agreements with downstream vendors and suppliers, internal service level agreements, new personnel and training and other mechanisms. Purchase requirements may be adjusted to account for Target Operational Service Levels. It is expected that programs will be required to monitor progress toward operational resilience. |
| 4.2 | Delivery Objectives: Service Delivery Objectives | Service Delivery Objectives must be defined for delivery of each Operations Critical and Business Critical service. | Once service dependencies have been identified and Target Operational Service Levels established, the Service Delivery Objectives can be defined for each critical service. These Service Delivery Objectives detail requirements for supporting systems of each critical service and how they can meet the impaired service targets and timeline in the defined set of Target Operational Service Levels. The Service Delivery Objectives provide the details of how quickly a service can be restored to a target impaired state with considerations of both business and technical dependencies. This may require new processes, mechanisms, systems and establishing agreements with third parties in addition to those established for normal service delivery. |

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 4.3 | Delivery Objectives: Data Restoration Objectives | Data Restoration Objectives must be defined to meet Service Delivery Objectives for each Critical Data Set component. | Data Restoration Objectives must be defined to meet the Service Delivery Objectives. If a service requires specific systems, applications, networks, configurations and business data, then all of those Critical Data Set components must be extracted at sufficient intervals, kept confidential, validated for integrity, made available and restored to the appropriate system within the required timeline to meet the Service Delivery Objectives for that critical service. Data Restoration Objectives should be maintained for each type of data and for the sensitivity level of the data.<br>Considerations include:<br>- Archive Environment and Mechanism<br>- Restoration Environment and Mechanism<br>- Mapping to Business Service, Systems, Applications<br>- Confidentiality - confidentiality requirements, processes and systems<br>- Integrity - validation and data integrity checks<br>- Availability - access, redundancy, distribution requirement<br>- Data Sensitivity<br>- Data Type<br>- Backup Interval - frequency of each type of extract (e.g.: full backup weekly, incremental daily)<br>- Time to Archive - time required to create the extract, transfer and validate in the archive environment<br>- Time to Restore - time required to transfer, validate and restore the extract to operations<br>- Business, Regulatory, Legal, Technical and other relevant policies<br>- Other |

## Step 5 – Preserve the Data Sets necessary to support Operations Critical and Business Critical services.

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 5.1 | Data Archive: Format | Critical Data Sets must be extracted in a format to meet Data Restoration Objectives. | The format should be defined for each Critical Data Set component. If data must be shared externally, then consideration must be given to ensure partners understand the format and can process the data. |
| 5.2 | Data Archive: Frequency | Critical Data Sets must be extracted at predefined intervals to meet Data Restoration Objectives. | Each data type may require a different backup frequency. For example, system images should change infrequently with the need to be extracted only upon change, but application data may require frequent full and incremental extracts. |
| 5.3 | Preservation: Confidentiality | Confidentiality of Critical Data Set extracts must be maintained using standard practices. | Critical Data Sets include business and user data as well as the applications, systems, networks, configurations and core infrastructure services required to restore critical services. When backing this data up, standard practices within the organization should be used to maintain confidentiality. It is important to consider confidentiality mechanisms both logical and physical which minimize the risks associated with both storing and restoring the data.<br>In a recovery situation, availability and integrity are often the primary considerations. Confidentiality should be maintained, but not at the expense of availability and integrity. |
| 5.4 | Preservation: Integrity | Critical Data Set extracts must be validated for integrity and completeness. Validation failures must be remediated. | Critical Data Sets include business and user data as well as the applications, systems, networks, configurations and core infrastructure services required to restore critical services. When backing this data up, standard practices within the organization should be used to validate and maintain integrity at each step of the process. Failures identified during validation must be remediated through a standard process or mechanism. |
| 5.5 | Preservation: Availability | Critical Data Set extracts must be distributed to provide redundancy and availability. | The following is a list of attributes to be considered when distributing data set extracts to provide redundancy and availability:<br>- number of instances number<br>- environment (e.g.: managed environment, single-tenant cloud, multi-tenant cloud)<br>- network segmentation<br>- physical/geographic separation<br>- data type (e.g.: business data, application data, user data, system image, configuration script, configuration file, etc.)<br>- archive type<br>- archive custodian<br>- data sensitivity / risk assessment |

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 5.6 | Preservation: Secure Archive Transfer | Critical Data Set extracts must be securely transferred to the archive environment at predefined intervals to meet Data Restoration Objectives. | Data Restoration Objectives must be defined to meet the Service Delivery Objectives. If a service requires specific systems, applications, networks, configurations and business data, then all of those Critical Data Set components must be extracted at sufficient intervals and securely transferred to the archive environment at redefined intervals to meet the Data Restoration Objectives. Archive processes should be monitored to ensure transfers are completed. |
| 5.7 | Preservation: Permanency | Critical Data Set extracts must be maintained on immutable storage. | Critical Data Sets include business and user data as well as the applications, systems, networks, configurations and core infrastructure services required to restore critical services. Data should be backed up to effectively immutable storage to ensure integrity is maintained. |
| 5.8 | Preservation: Retention | Critical Data Set extracts must be retained for a predefined length of time to meet Data Restoration Objectives. | Critical Data Sets include business and user data as well as the applications, systems, networks, configurations and core infrastructure services required to restore critical services. In order to meet Service Delivery Objectives, data should be retained for the time specified by the Data Restoration Objectives. |
| 5.9 | Preservation: Deletion | Multiple authorization must be enforced for deletion or destruction of Critical Data Set extracts. | Data must be preserved in accordance with organizational policies and Data Restoration Objectives. Critical Data Extracts should not be deleted or destroyed outside of established processes. Multiple authorization reduces the risk of unauthorized or unintentional deletion or destruction. |

**Step 6 – Implement processes to enable recovery and restoration of Operations Critical and Business Critical services to meet Service Delivery Objectives.**

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 6.1 | System Recovery and Reconstitution: Recovery Environment | The recovery environment, processes and mechanisms must be sufficient to meet Service Delivery Objectives. | The recovery environment and restoration mechanisms must be aligned to the Service Delivery Objectives to meet the Target Operational Service Levels including target impaired states. The recovery environment to establish an impaired service level may be separate from the full-service restoration environment to enable the organization to quickly achieve the defined Target Operational Service Levels while full restoration of services work is ongoing. |
| 6.2 | System Recovery and Reconstitution: Restore Critical Data | Data restoration processes and mechanisms must be sufficient to restore the Critical Data Set Archive into the designated recovery environment. | Processes and systems must be designed and tested to meet requirements. The restoration should be highly automated and the length of time for restoration should be known and periodically tested. |
| 6.3 | Archive Access: Access Redundancy | Redundancy must be established for authorized access to archives. | Access must be granted to more than one identity to reduce risk. Procedures and mechanisms must provide redundancy for authorized access to archives.<br>While redundancy is critical to ensure access during a crisis, consideration must also be given to protect sensitive data. Access should be limited. |
| 6.4 | Cryptographic Protection: Key Management | Cryptographic keys must be available for restoration processes. | The organization must establish effective procedures or mechanisms to ensure key availability for restoration processes. |
| 6.5 | Cryptographic Protection: Key Acceptance | Archive restoration systems and cryptographic systems must be available to accept cryptographic keys from authorized users. | |
| 6.6 | Response Planning: Incident Response Plan | Incident Response plans must be reviewed at least annually and updated as required to address the risk of disruption or impairment to Operations Critical and Business Critical services. | Recommended frequency is at least annually or upon significant change. |

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 6.7 | Response Planning: Recovery Plan | Recovery Plans must be reviewed at least annually and updated as required to address disruption or impairment to Operations Critical Services and Business Critical Services. | Recovery plans should include considerations for Target Operational Service Levels and include transitions between predesigned impaired states.<br>Recommended frequency is at least annually or upon significant change. |
| 6.8 | Response Planning: Communications Plan | Communications plans must be updated to include required communications to stakeholders, customers, partners and counterparties in the event of disruption or impairment to Operations Critical and Business Critical services. | Communications plans should include both required internal communications as well as external communications to customers, partners, counterparties, third-parties, suppliers, law enforcement, government, regulators and other stakeholders.<br>Communications plans should include considerations for operating at Target Operational Service Levels, transitions between target impaired states and for situations where target service levels cannot be met.<br>Communications Plans should include templates to inform and manage expectations of customers, partners and counterparties in the event of a service disruption or impairment. |

## Step 7 – Independently evaluate design and test periodically.

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 7.1 | Evaluation: Independence | The policies, architecture and design of Operational Resilience processes and mechanisms must be evaluated periodically by a group independent of the design team. | Periodic review should be conducted by a team independent of the team responsible for the architecture and design, including the policies, organizational supports, business processes and technical mechanisms. Independence may be achieved within the same organization (e.g.: through an internal audit function) or using an external evaluator. |
| 7.2 | Testing: Independence | Operational Resilience processes, mechanisms and configurations must be tested by a group independent of the implementation team to confirm achievement of operational effectiveness and adequacy to meet Service Delivery Objectives. | Periodic testing should be conducted by a team independent of the team responsible for the ORF implementation. Independence may be achieved within the same organization (e.g.: through an internal team) or using an external evaluator.<br>Comprehensive testing may include third-parties and full cutover tests. |
| 7.3 | Monitoring: Coverage and Effectiveness | Implementation of Operational Resilience Framework rules must be monitored to ensure they provide adequate coverage and effectiveness. | Implementations should be instrumented and monitored where possible to measure coverage and effectiveness and alert when there are gaps. For instance, if a validation test failed, the team responsible for monitoring performance of the ORF should be alerted to the failure, even if it is automatically remediated. |
| 7.4 | Training and Exercises: Testing, Training and Exercises | The organization must establish an Operational Resilience Testing, Training and Exercises program to include involvement of management and operations teams. | Operational Resilience testing, training and exercises may be achieved by enhancing existing Cybersecurity, Business Continuity and Disaster Recovery programs within the organization to include Operational Resilience. Exercises should be conducted periodically across people, process and technology and at appropriate organizational levels to include executive management, business leadership, legal, technical support teams and ORF Operations Teams. Incident Response Plans, Recovery Plans and Communications Plans should be included in the exercise program. Exercises should include plausible scenarios that may cause significant service disruptions, even if they are unlikely. |
| 7.5 | Continuous Improvement: Changes | Operational Resilience policies, processes and mechanisms must be updated to address changes to the sector, organization, business, information systems, ecosystem and environment of operation. | The organization must regularly review and adapt policies, processes and mechanisms to account for any changes in various aspects such as the sector it operates in, the environment in which it operates, the organization itself, its business operations, the information systems, third-parties and suppliers, the larger ecosystem, and the changing needs of customers, business partners and counterparties. This proactive approach ensures that the organization's operational resilience remains effective and can respond to evolving challenges and threat in a dynamic business landscape. |

| ID | Topic: Sub-Topic | Rule Statement | Rule Notes |
|---|---|---|---|
| 7.6 | Continuous Improvement: Problems | Problems encountered during implementation, execution, incident response, exercises, or testing of Operational Resilience policies, processes and mechanisms must be addressed. | Issues or challenges that arise during the implementation, execution, incident response activities, exercises or testing must be acknowledged and resolved. This includes identifying and rectifying problems or deficiencies in the implementation to ensure it functions effectively. |

## Appendix 2 - References

The Operational Resilience Framework builds upon past IT and cybersecurity control frameworks and regulatory guidance. The following is a list of references for those materials, ordered by title:

"Business Continuity Management." FFIEC IT Handbook InfoBase. FFEIC, November 2019.
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx.

"Cybersecurity Framework." NIST. NIST, February 12, 2014.
https://www.nist.gov/cyberframework.

"Discussion Paper - Bank of England." Bank of England, Prudential Regulations Authority, Financial Conduct Authority, July 2018.
https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A.

"Effective Practices for Cyber Incident Response and Recovery." Financial Stability Board, April 20, 2020.

"ISO 22301:2019." ISO. ISO, October 30, 2019.
https://www.iso.org/standard/75106.html.

"ISO/IEC 27001 - Information Security Management." ISO. ISO/IEC, April 3, 2020.
https://www.iso.org/standard/27001.

"ISO/IEC 27002:2013." ISO. ISO/IEC, March 26, 2018.
https://www.iso.org/standard/54533.html.

"ISO/IEC 38505-1:2017." ISO. ISO/IEC, January 15, 2022.
https://www.iso.org/standard/56639.html.

"ISO/IEC TR 38505-2:2018." ISO. ISO/IEC, May 16, 2018.
https://www.iso.org/standard/70911.html.

"ISO/IEC TS 38505-3:2021." ISO. ISO/EIC, December 20, 2021.
https://www.iso.org/standard/56643.html.

AXELOS. *ITIL Foundation ITIL 4 Edition*. Norwich, England: The Stationery Office, 2019.

"Operational Resilience: Impact Tolerances for Important Business Services." Bank of England, Financial Conduct Authority, March 2021.

"Principles for Operational Resilience." Basel Committee on Banking Supervision, Bank For International Settlements, March 2021.

Ross, Ron, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, and Gary Guissanie. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." NIST. NIST, January 28, 2021. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

Joint Task Force. "Security and Privacy Controls for Information Systems and Organizations." NIST. NIST, December 10, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

"Sound Practices to Strengthen Operational Resilience." FDIC, The Board of Governors of the Federal Reserve System, and The Office of the Comptroller of the Currency, October 30, 2020.

Swanson, Marianne, Pauline Bowen, Amy Phillips, Dean Gallup, and David Lynes. "SP 800-34 Contingency Planning Guide for Federal Information Systems." NIST-CSRC. NIST, November 11, 2010. https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final.

"The 18 CIS Controls." CIS. CIS, October 28, 2021. https://www.cisecurity.org/controls/cis-controls-list.

[1] https://www.strategy-business.com/article/8375
[2] https://www.pwc.com.au/risk-controls/enterprise-resilience.html
[3] https://www.gartner.com/en/information-technology/glossary/operational-resilience
[4] https://www.techtarget.com/searchdisasterrecovery/definition/operational-resilience