Business Resilience Council

by Global Resilience Federation

Operational Resilience Framework

Rules – Version 1.0

ORF

October 2022

Key Contributors

Special thanks to the volunteer team of industry professionals and subject matter experts who have contributed significant time and energy to this effort.

ORF Chairman

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

ORF Task Force

- Bob Blakley, Operating Partner, Team8
- Jon Washburn, Chief Information Security Officer, Stoel Rives LLP
- Alex Sharpe, Sharpe Management Consulting
- Dr. Georgianna Shea, Chief Technologist, Foundation for Defense of Democracies
- Charles Blauner, Operating Partner, Team8
- Simon Chard, Managing Director, S&P Global
- Susan Rogers, Executive Director Operational Resilience, SMBC
- Jennifer Buckner, SVP Technology Risk Management, Mastercard
- Judy Erbs, VP Technology Risk Management, Mastercard

GRF Staff

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

Additional Reviewers (last updated 10/12/2022):

- Paul Williams, Phoenix Resilience LTD, Former Division Head at Bank of England
- Michael Daniel, CEO, Cyber Threat Alliance
- Adam Stage, Sr Manager Operational Resilience, TSB UK
- Annie Fixler, CCTI Deputy Director, Foundation for Defense of Democracies
- Greg Gist, Director of Risk Management, IBM Promontory Financial Group
- Linda Betz, Information Security Consultant, FS-ISAC
- Rock Lambros, CEO and Founder, RockCyber

NOTE: The additional reviewers list may be updated without iterating the rules version number once permission is received from the many representatives across multiple industries that provided direct feedback which helped shape the framework. Appearing on the reviewers list does not serve as an endorsement of the ORF by the parent company.

Contents

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 three 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.

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.

Executive Summary

Operational resilience is the ability to reliably provide critical services in the face of any disruption. Since the release of the July 2018 Bank of England discussion paper, "*Building the UK financial sector's operational resilience*," regulatory bodies, trade association alliances, and individual institutions 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 which have been insufficient in the past, especially in the face of destructive events such as ransomware, wiperware, and data center fires.

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.

The goal of the ORF working group is to develop and refine an industry-driven framework of rules. These rules provide continuity and recovery of critical data, systems and processes required to minimize service disruptions to customers, partners and counterparties. 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 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 during a six-month period ending in September 2022. 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 would like to personally thank the Chairman of the ORF, Trey Maust, the dedicated task force, and all who have contributed to this effort so far. 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 accessible to organizations of all sizes, shapes, and across all sectors. 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. The focus of Sheltered Harbor was to protect consumers and public confidence in the banking system by creating a standard mechanism to generate immutable backups to enable recovery of a specific set of consumer data. If a bank's systems were erased or destroyed, the data could be recovered. The impact of this single set of services gives customers the confidence that their deposit, retail, brokerage, and asset management account balances are preserved, and that they can access their funds irrespective of the nature and severity of the hazard that caused the outage.

In 2018, the Bank of England released a paper entitled "*Building the UK financial sector's operational resilience*" which highlighted how operational resilience was important in the banking sector to prevent systemic impacts. The paper included the statement, "The financial sector needs an approach to operational risk management that includes preventative measures and the capabilities – in terms of people, processes and organizational culture – to adapt and recover when things go wrong." This paper kicked off a firestorm of working groups at large financial institutions across the globe. These efforts were supplemented by task forces and committees and ultimately by supervisory reviews from regulators at large institutions.

Since the publication of that paper, regulators in the US and Europe have provided principles and guidance for operational resilience. In October 2020, the United States Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation issued an interagency paper titled "*Sound Practices to Strengthen Operational Resilience*." It is clear there is a new spotlight on operational resilience, with a focus on critical services provided by businesses to customers, partners and counterparties.

The guidance provided by regulators includes a few key activities. The first is continuity of critical services and documenting what is required to deliver each critical service. The second is identifying the maximum levels of disruption that can be tolerated by consumers of the services. And the third is building resilient business services, assuming disruptions will occur. However, there are some key gaps in most organizations' Business Continuity and Disaster Recovery planning: most of those efforts are focused on recovering business data only and do not provide mechanisms to operate in an impaired state during a crisis.

Today, Sheltered Harbor is widely adopted in the US financial sector, but it is also incomplete. There is not just a need to protect a small set of consumer data but to widely enable the operation of critical services in the face of significant disruptive events, across sectors, even if they need to be run in an impaired state. It is important to not only recover business and consumer data, but to also recover the systems, networks, applications, and configurations that are required to quickly get critical services operating again, preventing further systemic impacts and harm to the broader ecosystem.

In 2021, Global Resilience Federation initiated the effort to develop the Operational Resilience Framework (ORF) rules with support from subject matter experts and professionals across several industries. The mission statement for this activity is as follows:

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.

Using the framework, an organization develops a clear understanding of its most important Business Critical and Operations Critical services, a comprehensive understanding and mapping of the systems and processes needed to support those services, knowledge of how the failure of individual systems or processes could impact the delivery of those services, and knowledge of which services are capable of being substituted. That's a very important element, because operational resilience does not require bringing the original system back online, or even with the same capacity. It is about delivering a service in a degraded state, possibly using an alternate processing site and alternate method to deliver the service. This framework also ensures plans are tested effectively including both communications within the organization and external communications to customers, partners, counterparties, law enforcement and other stakeholders.

The rules were developed by industry in alignment with existing cybersecurity and IT controls from NIST, ISO, ITIL and others. These rules are not meant to be overly prescriptive, but provide the framework and supports for organizations of any size and shape to build operational resilience into their services and to weave the fabric of resilience into our broader, interdependent and interconnected ecosystem. The rules have been publicly reviewed and testing has been initiated in several corporate environments. The rules in the framework and the implementation aids will be continually improved with support from members of the BRC, and from independent implementers providing feedback, to become the new standard for operational resilience.

Path to Operational Resilience

This document was written for executives, risk management and business continuity management professionals, and both business-aligned and technology-aligned operational resilience practitioners. The ORF has seven key steps in the path to operational resilience. These steps were developed in a sequence starting with foundational risk management, cybersecurity and information technology controls. The intent is for an organization to review the steps and consider them in the context of their business and build their own plan of implementation from them.

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.

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.

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 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.

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.

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 can process up to 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.

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.

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.

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.

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 Rules V1.0 – 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.

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 available, organized by the steps in the ORF Path to Operational Resilience. The development effort for these aids is ongoing.

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 continued support from industry, government, and regulatory bodies, and with contributions from the members of GRF's Business Resilience Council, the Operational Resilience Framework rules will be reviewed annually and updated as required. The implementation aids in the section above will be developed, reviewed, published and updated periodically. Products and supporting documents will be developed to simplify adoption and support implementation by organizations of any size. We are looking for support for all of these efforts. Please reach out at orf@grf.org to volunteer for our working groups. Please also consider joining the BRC to support these activities and receive the many benefits of membership in an all-hazards, multi-sector collective defense community that includes vendors and suppliers to enhance resilience.

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.

White Paper on Effective Testing of Operational Resilience: Testing and exercises are a difficult and challenging proposition for any organization. For this reason, we will be developing a white paper to provide specific and comprehensive guidance on how to run a OR testing program, who should be involved, and provide examples and starting places for tests and exercises.

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.

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

Maturity Ladder: With support from the Business Resilience Council and the existing ORF working group, a maturity ladder will be developed to guide organizations through the process of implementing the ORF and advancing the maturity of their Operational Resilience programs.

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 or other supports that will foster adoption and ease implementation of the ORF, please send them to orf@grf.org. Additionally – please share your experiences and help us develop case studies – we will keep all submissions anonymous unless otherwise specified by the author.

Appendix 1 - Rules

The following are the Operational Resilience Framework Rules – Version 1.0.

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 industry-recognized risk management, information technology and cybersecurity control frameworks.	A foundational step in development of Operational Resilience is to establish primary risk management practices, information technology and security controls and related policies and practices 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. All changes to ORF-related 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 (eg: NIST SP 800-53), and the International Organization for Standardization (eg: 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 as a key role with ownership and accountability for implementation of Operational Resilience within the organization. This executive should 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. 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: Service Catalog	Business services must be inventoried.	External business service must be inventoried to ensure full coverage in operational resilience implementation. Supporting processes, systems, data sets, and service dependencies must also be identified prior to operational resilience implementation, but these may be detailed at a later step in the process. The core activity requires business executives to inventory the organization's services at a high level to enable further analyses.
2.2	Ecosystem: 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: 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. 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: 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: Service Delivery	The supporting processes required for delivery of Operations Critical and Business Critical services must be identified.	Each critical service must be mapped to identify internal processes and business dependencies supporting delivery of the service.
3.2	Minimum Viable Service: 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. 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. 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: Minimum Service Levels	Minimum Viable Service Levels must be established for each customer, partner and counterparty group.	To better understand minimum viable service levels, the organization may perform customer surveys, testing, and analysis. 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. The goal is to create a distinct set of minimum service levels for each critical service 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.

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 Dependencies	Internal and External dependencies must be identified for delivery of each Operations Critical and Business Critical service.	Service Design - Document how each critical service is delivered including people, processes, technologies, third and fourth-party vendors, suppliers, and other dependencies. 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:** **People:** - Business Unit / Organizational Dependencies **Process:** - Payment Processing - Line of Business Processes **Technology:** - Custom Hardware or Software - Data Centers - Cloud Providers - Servers, Applications, Networks, Configurations **Nth-Party:** - Third-Party Service Providers - Third-Party Equipment Providers - Component / Materials Providers - Ecosystem Sector and Cross-Sector dependencies - Ecosystem Regional, National, Global dependencies - Other Supply Chain dependencies **Customers, Partners and Counterparties:** - Customer, Partner and Counterparty agreements - Readiness to receive service
4.2	Delivery Objectives: Service Design	Target Operational Service Levels must be established to include considerations of minimum service levels required by customers, partners and counterparties and identified service dependencies.	Service design may require updates to account for considerations of minimum 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. 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. It is expected that programs will be required to monitor progress toward operational resilience.

ID	Topic:Sub-Topic	Rule Statement	Rule Notes
4.3	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.
4.4	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. Considerations include: - Archive Environment and Mechanism - Restoration Environment and Mechanism - Mapping to Business Service, Systems, Applications - Confidentiality - confidentiality requirements, processes, and systems - Integrity - validation and data integrity checks - Availability - access, redundancy, distribution requirement - Data Sensitivity - Data Type - Backup Interval - frequency of each type of extract (eg: full backup weekly, incremental daily) - Time to Archive - time required to create the extract, transfer, and validate in the archive environment - Time to Restore - time required to transfer, validate, and restore the extract to operations - Business, Regulatory, Legal, Technical, and other relevant policies - 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.	
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.
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: - number of instances - environment (eg: managed environment, single-tenant cloud, multi-tenant cloud) - network segmentation - physical separation - data type (eg: business data, application data, user data, system image, configuration script, configuration file, etc.) - archive type - archive custodian - data sensitivity / risk assessment
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 predefined intervals to meet the Data Restoration Objectives. Archive processes should be monitored to ensure transfers are completed.

ID	Topic:Sub-Topic	Rule Statement	Rule Notes
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 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 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.
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.
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 Management	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 Services and Business Critical Services.	Recommended frequency is at least annually or upon significant change.
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.	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. 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 ORF 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 (eg: through an internal audit function) or using an external evaluator.
7.2	Testing: Independence	ORF 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 (eg: through an internal team) or using an external evaluator.
7.3	Monitoring: Coverage and Effectiveness	Implementation of ORF 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. The Operational Resilience Testing, Training, and Exercise program may leverage existing functions within the organization.
7.5	Continuous Improvement: Changes	ORF policies, processes, and mechanisms must be updated to address changes to the sector, organization, business, information systems, ecosystem, or environment of operation.	Changes to the ecosystem includes changes to the needs of customers, business partners, and counterparties.
7.6	Continuous Improvement: Problems	Problems encountered during implementation, execution, incident response, exercises, or testing of ORF policies, processes, and mechanisms must be addressed.	

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/isoiec-27001-information-security.html.

"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.