





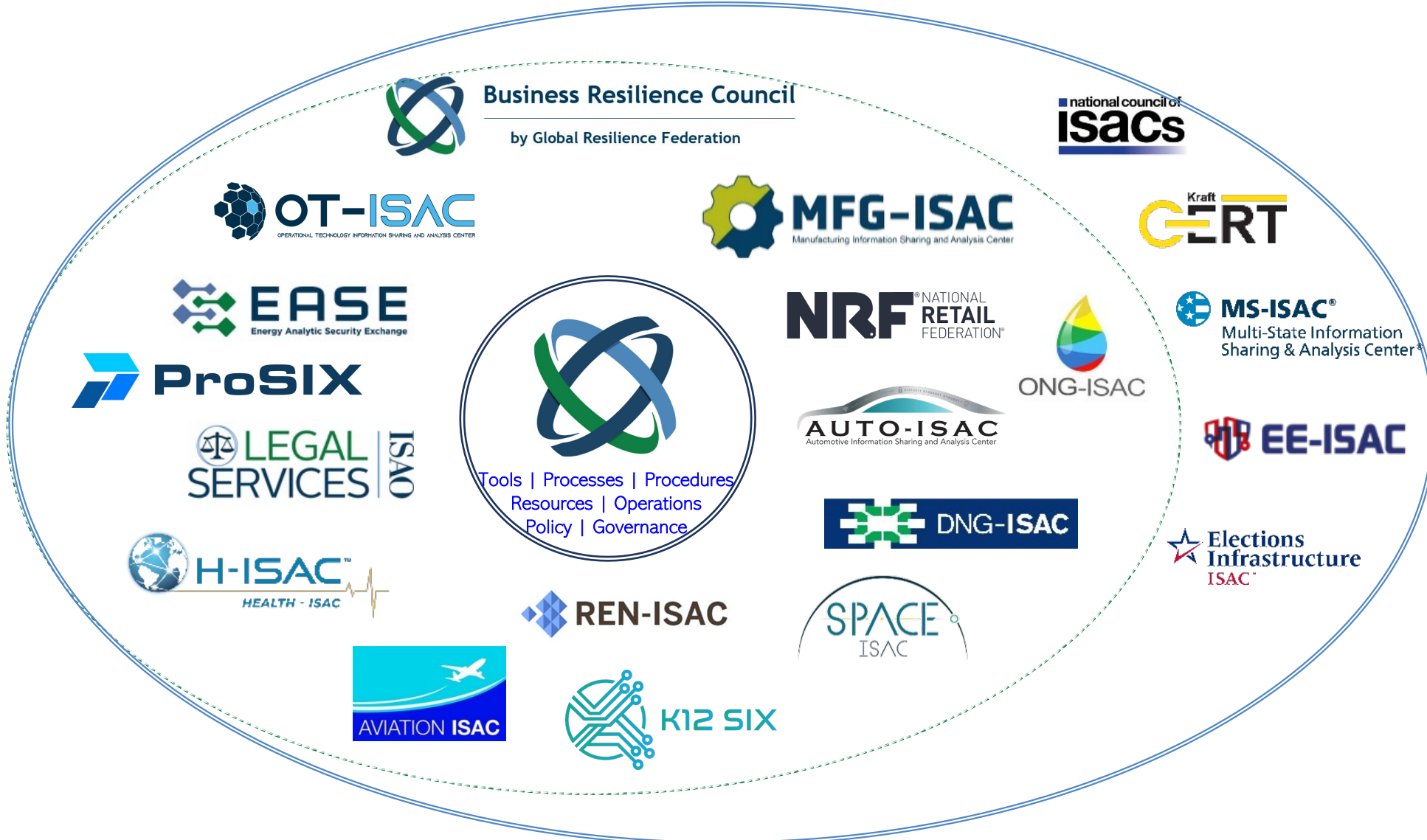


Building Operational Resilience: A Framework and its Implementation

BRC Overview - Agenda

-  **Introduction**
-  **Understanding the ORF**
-  **Key Components and Real World Implementation**
-  **Call to Action**
-  **Closing Remarks**
-  **Q&A Session**

Introduction – Who Is GRF?



Introduction – What is Operational Resilience



Operational Resilience - The level of continuity and recoverability of critical data, systems, and business processes required to limit service disruptions to customers, partners and counterparties.



Introduction – Why Operational Resilience Now

Winter Storm Uri 2021 The Economic Impact of the Storm

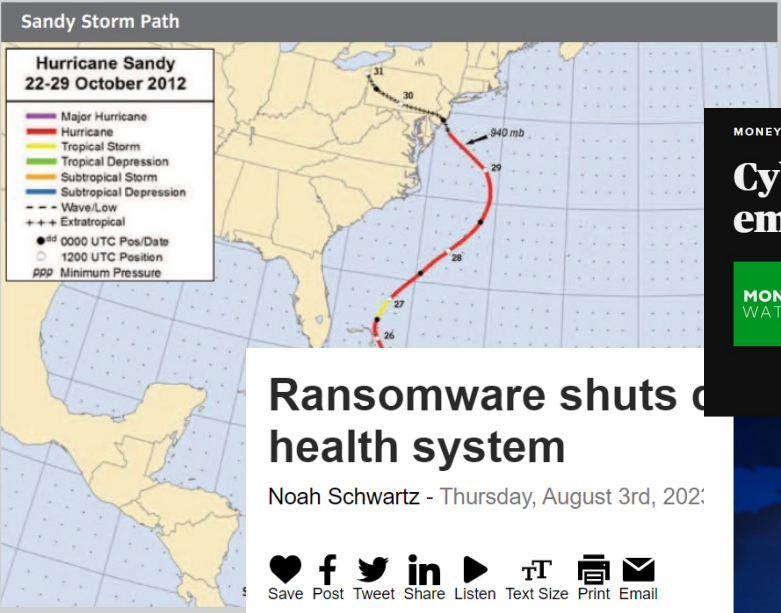


Administration | Priorities | The Record | Briefing Room | Español | MENU



link its closing to a ransom... SHARE & SAVE - f t e ...

HOME / FEATURED / EDUCATION / HURRICANE



Sandy by the Numbers
Sandy made landfall three times in Cuba, Cuba, on October 25, 2012.
The storm's wind speed peaked at 140 mph.
Its wind field extended for 1,000 miles.
In the US, \$50 billion in damage was caused, making it more costly than Hurricane Katrina in 2005.

Ransomware shuts down health system

Noah Schwartz - Thursday, August 3rd, 2023



A cyberattack at Manchester-based Eastern Cheshire and Northern Lancashire NHS Foundation Trust emergency room diversions, *NBC Connecticut*

According to the health system's website, the attack affected all emergency departments, specialty care locations, the dental services, and other facilities, ECHN's parent company, according to the health system's website.

The FBI is currently investigating the attack.

"It was a ransomware attack," Jillian Menzel, ECHN's chief information officer, said. "We have a prospect team that is working on that currently." national command center that is working on that currently."

The issue affected the emergency rooms at both ECHN hospitals and caused ECHN to divert patients.

The health system is reaching out to patients whose appointments were affected by the incident.

MONEYWATCH
Cyberattack emergency room diversions
BY KHRIS...
UPDATED...

ALL ABOUT ANN ARBOR

Ken Haddad, Digital Content Manager
Published: August 29, 2023 at 10:09 AM
Updated: August 29, 2023 at 10:19 AM
Tags: University Of Michigan, Ann Arbor

Sign up for our Newsletters

Enter your email here!



University of Michigan shuts down internet due to security concern

'It may be several days before all online services return to their normal levels'



University of Michigan (WDIV)



Operational Resilience Framework – Origin Story

BANK OF ENGLAND **FCA** FINANCIAL CONDUCT AUTHORITY

Discussion Paper

Building the UK financial sector operational resilience

- | Bank of England DP01/18
- | Prudential Regulation Authority (PRA) DP01/18
- | Financial Conduct Authority (FCA) DP18/04

July 2018

FSB FINANCIAL STABILITY BOARD

Effective Practices for Cyber Incident Response and Recovery

Consultative Document

20 April 2020

FDIC

Home // News // Press Releases // 2020

Press Release

Agencies Release Paper on Operational Resilience

October 30, 2020

For release at 4:45 p.m. EDT

Federal bank regulatory agencies today released a paper outlining sound practices designed to help large banks increase operational resilience. Examples of risks to operational resilience include cyberattacks, natural disasters, and pandemics.

The "Sound Practices to Strengthen Operational Resilience" paper outlines practices to increase operational resilience that are drawn from existing regulations, guidance, statements, and common industry standards. The practices are grounded in effective governance and risk management

risks, and include resilient information systems or guidance.

banks with more than \$250 billion in total assets and other risk characteristics

[Operational Resilience](#)

[When Operational Resilience](#)

BANK OF ENGLAND **FCA** FINANCIAL CONDUCT AUTHORITY

Building operational resilience: Impact tolerances for important business services

Bank CPs relating to FMIs | Bank of England (Bank)
CP29/19 | Prudential Regulation Authority (PRA)
CP19/32 | Financial Conduct Authority (FCA)

Basel Committee on Banking Supervision

Principles for Operational Resilience

March 2011

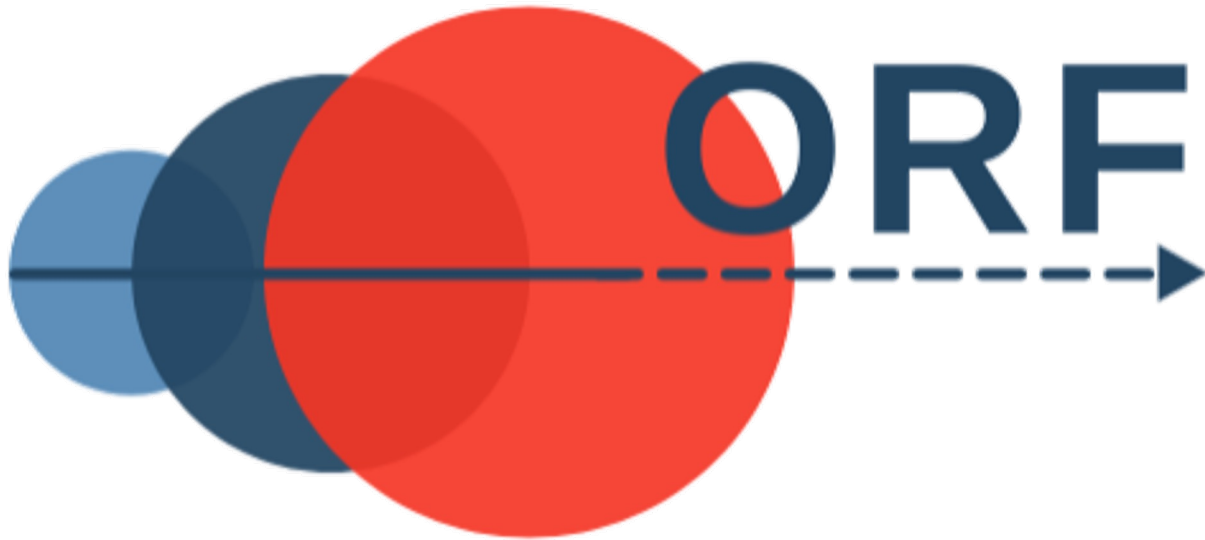
BANK FOR INTERNATIONAL SETTLEMENTS

Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					
Degree of Dependency	Technology			People	
	Process				

Why are there so few things here?
Is industry actually solving the right problems?





Purpose- To develop and refine an industry-driven framework of rules, supported by architecture and controls, 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.

Operational Resilience Framework

ID	Rule Statement	Rule Notes
1.0		
1.1	The organization must implement an industry-	A foundational step in development of Operational Resilience is to establish primary information technology and

Assessments

- Step 1 - Build the Foundation
 - Governance
 - 1.1 Security Controls
 - 1.2 Executive Sponsorship
 - 1.3 Sustainability
- Step 2 - Understand the Ecosystem
- Step 3 - Identify Minimum Viable Service Levels
- Step 4 - Define Service Delivery Objectives
- Step 5 - Preserve the Data
- Step 6 - Enable Recovery
 - System Recovery and Reconstitution
 - Archive Access
 - Cryptographic Protection
 - Response Planning
- Step 7 - Independently Test

Category 1 of 7 in ORF Demo 2

Process 1 of 1 in Step 1 - Build the Foundation

Attribute 2 of 3 in Governance

Back Skip Save And Continue

Based upon your observations, which of the following statements below most accurately describes the current state of your organization's **1.2 Executive Sponsorship** as it relates to **Governance**?

Select an answer that applies to 1.2 Executive Sponsorship:

- Not Implemented:** A qualified executive is not designated as responsible or accountable to ensure appropriate organizational support for operational resilience
- Partially Implemented:** A qualified executive is occasionally designated as responsible or accountable to ensure appropriate organizational support for operational resilience.
- Implemented:** A qualified executive is designated as responsible and accountable to ensure appropriate organizational support for operational resilience

Supporting Artifacts

Attach Files OneDrive

ORF Demo 2 3% Complete

33% Complete

Governance 33% Complete

Subject: Governance

Context: 1.2 Executive Sponsorship

Additional Details

DESCRIPTIONS

1.2 Executive Sponsorship
Designate a qualified executive as both responsible and accountable to ensure appropriate organizational support for operational resilience.
Responsible: Operational Resilience Executive, Business Leaders, Technology Leaders

Governance
The process of overseeing the control and direction of an organizations policies and procedures.

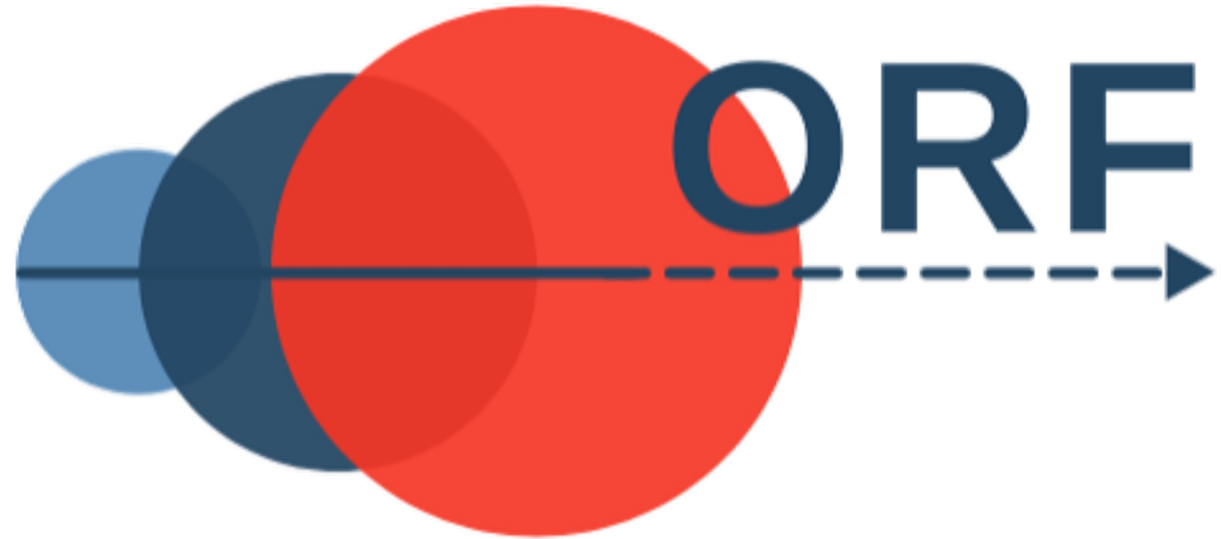
CONTROL MAPPINGS

Skip Save And Continue



Key Principals:

- Distributed and Immutable Backups
- Leadership: Operational Resilience Executive
- Minimum Viable Service Levels
- Service Delivery Objectives
- Operations/Business Critical Services
- Expanded Definition of Critical Data Sets



Path to Operational Resilience

1. Implement an industry-recognized IT and Cybersecurity control framework.
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.



Key Components of the Framework

Foundation

Ecosystem

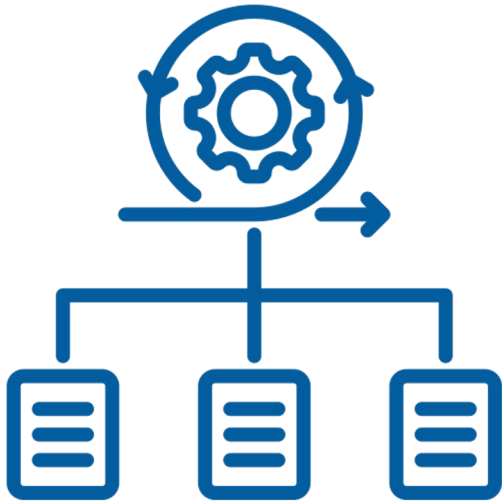
Service Levels

Delivery Objectives

Preserve Data

Enable Recovery

Independently Test



Cyber and Risk Management



Leadership



Sustainability



Key Components of the Framework

Foundation

Ecosystem

Service
Levels

Delivery
Objectives

Preserve
Data

Enable
Recovery

Independently
Test

Financial Sustainability:

Lost Revenue = \$250M ARR x .5 / 12 Mo = **\$10.4M,**

+ Damages: Avg Cost of a ransomware attack(\$4.83M) = **\$15.23M**

X Risk Assumptions: \$15.23M X .05 (1/20 years)

Acceptable Annual Budget = **\$761.5K**

Cost of 1 Operational Critical Service Resilience: ~ 40K



Key Components of the Framework- 2nd Step

Foundation

Ecosystem

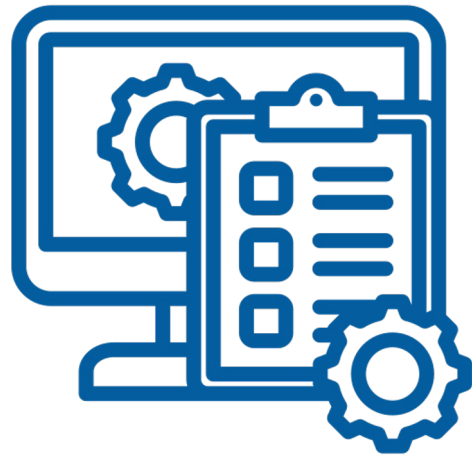
Service Levels

Delivery Objectives

Preserve Data

Enable Recovery

Independently Test



**Inventory of
Business Services**



**Criticality of
Services Determined**



**Customers Groups
Defined**



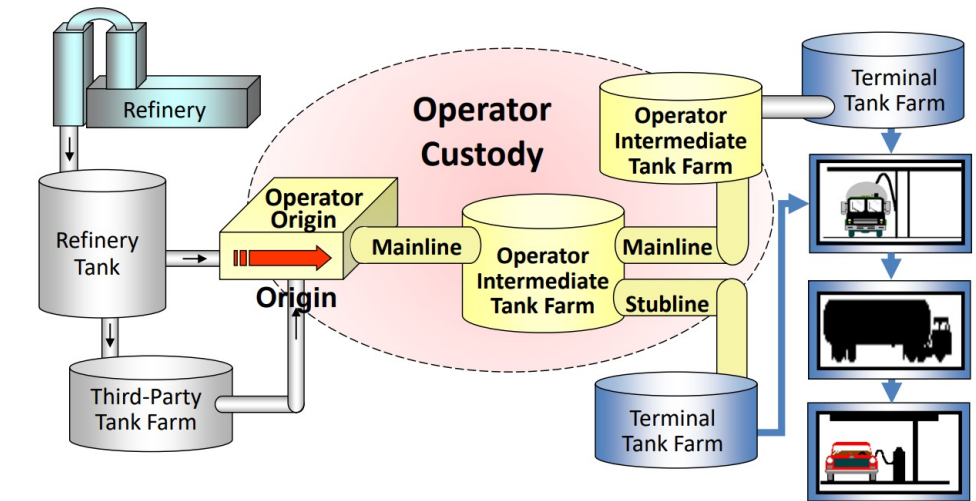
**Customers Groups
Prioritized**



ORF – ACME Pipeline Service Criticality

Foundation	Ecosystem	Service Levels	Delivery Objectives	Preserve Data	Enable Recovery	Independently Test
------------	-----------	----------------	---------------------	---------------	-----------------	--------------------

ACME PIPELINE CO.		Services	Service Description	Crit
RACI		Oil/Product Delivery	Customer facing, delivery/tracking of products (including Shipping)	
C-Suite		Testing	Regulator required for safe transport of Oil Products	
A	Operational Resilience Exec	Billing	The ability to send and receive invoices	
R	Business Leaders			
C	Contingency Planners	Product Acquisition/ Consignment	Acquiring product to transport through pipeline	
	Technology Leaders			
C	Implementation Team	Payroll	Paying Employees	
		Comms	For internal and external communication of all kinds	



Operations Critical – Operations critical components are data, systems and processes that require near-continuous functioning to limit service disruptions and impacts to customers, business partners and other counterparties.

ORF – ACME Customer Priority

Foundation		Ecosystem	Service Levels	Delivery Objectives	Preserve Data	Enable Recovery	Independently Test
ACME PIPELINE CO.		Group Name	Number of Customers	Summer Daily Revenue	Group Vulnerability	Group Priority	
RACI		Airports	7+				
	C-Suite	Consumer Gas Stations	300,000+				
A	Operational Resilience Exec						
R	Business Leaders	Commercial/Trucking Gas Stations	30,000				
R	Contingency Planners						
	Technology Leaders	Consumers of other Petroleum Products	2,000				
	Implementation Team						

Key Components of the Framework- 3rd Step

Foundation

Ecosystem

Service Levels

Delivery Objectives

Preserve Data

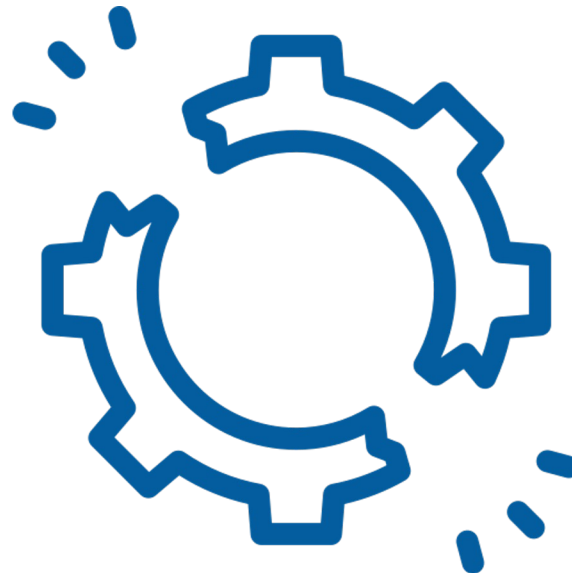
Enable Recovery

Independently Test

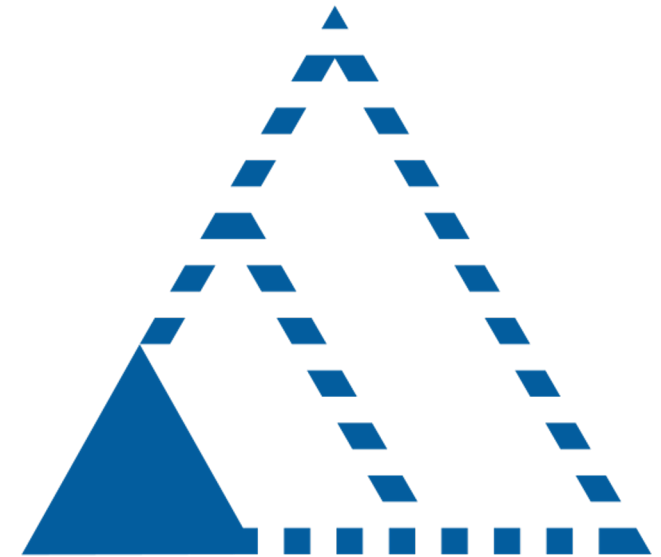
Define the Minimum Viable Service Levels for each Operations Critical and Business Critical service.



Supporting processes for service delivery identified



Identify when and how a service breaks



Establish Minimum Viable Service Levels




ORF – ACME FI Minimum Viable Service Levels

Foundation		Ecosystem	Service Levels	Delivery Objectives	Preserve Data	Enable Recovery	Independently Test
RACI		MVSL	Level 1	Level 2	Level 3	Level 4	
I	C-Suite	Target Service Level	High priority customers receive near normal service, Low and medium priority customers receive delayed service.	HP customers receive delayed service, MP receive significantly delayed service. LP customers are instructed to use an alternate method.	HP customers receive significantly delayed service, LP and MP are instructed to use an alternate method with assistance.	All customers are assisted in using an alternate method. Priority still dictates level of support.	
A	Operational Resilience Exec						
R	CFO/Treasury Management						
R	CRO						
R	Business Leaders	Impacts and Outrage	All customers partially satisfied – minor impacts	All customers struggling – significant impacts	Low priority customers outraged	Low and Medium priority customers outraged	
R	Contingency Planners	Delivery Priorities	>80% normal Transaction to all customers	>60% normal deliveries to all customers Rest shunted to alternative method	>40% normal deliveries to High and Medium priority customers Rest shunted to alternative method	0% normal deliveries High priority customers shunted to alternative method	
C	Technology Leaders						
I	Implementation Team						
	Critical Third-Parties	Estimated Transactions	7407	5555	3703	0	
C	Legal						



ORF – ACME Pipeline Minimum Viable Service Levels

Foundation		Ecosystem	Service Levels	Delivery Objectives	Preserve Data	Enable Recovery	Independently Test
		MVSL	Level 1	Level 2	Level 3	Level 4	
		Target Service Level	Limited level of product delivery to all customers, enabling near normal operations for 2 weeks	Significantly limited product delivery to all customers, enabling near normal operations for 4 weeks	Limited level of product delivery to High and Medium Priority customers, enabling near normal operations for 6 weeks	Limited delivery to High Priority Customers. Minimize mass panic and systemic impacts to critical infrastructure and the economy.	
RACI							
	C-Suite						
A	Operational Resilience Exec						
C	Business Leaders	Impacts and Outrage	All customers partially satisfied – minor impacts	All customers struggling – significant impacts	Low priority customers outraged	Limited Supply chain disruptions	
R	Contingency Planners						
C	Technology Leaders	Delivery Priorities	>80% normal deliveries to all customers	>60% normal deliveries to all customers	>50% normal deliveries to High and Medium priority customers	<50% normal deliveries to High priority customers	
C	Implementation Team						
		Estimated Deliveries	76,800,000 gal/day	57,600,000 gal/day	47,500,000 gal/day	37,500,000 gal/day	



Key Components of the Framework- 4th Step

Foundation

Ecosystem

Service Levels

Delivery Objectives

Preserve Data

Enable Recovery

Independently Test



Identify Dependencies for each service



Target Operational Service Levels




Service Delivery Objectives



Data Restoration Objectives



ORF – ACME Service Delivery Objectives

Foundation		Ecosystem	Service Levels	Delivery Objectives	Preserve Data	Enable Recovery	Independently Test
		MVSL	Level 1	Level 2	Level 3	Level 4	
		Delivery Priorities	>80% normal deliveries to all customers	>60% normal deliveries to all customers	>50% normal deliveries to High and Medium priority customers	>50% normal deliveries to High priority customers	
RACI							
	C-Suite						
A	Operational Resilience Exec	Estimated Deliveries	76,800,000 gal/day	57,600,000 gal/day	47,500,000 gal/day	37,500,000 gal/day	
C	Business Leaders	Service Design	<ul style="list-style-type: none"> - Restore Operations Critical functions - Local reserves - Manual process 	<ul style="list-style-type: none"> - Restore Operations Critical functions - Local reserves - Manual process - 3rd-Party delivery 	<ul style="list-style-type: none"> - Restore Operations Critical functions - Local reserves - Manual process - 3rd-Party delivery - Overtime/duty reassignment 	<ul style="list-style-type: none"> - Restore Operations Critical functions - Local reserves - Manual process - 3rd-Party and Govt delivery - Overtime/duty reassignment 	
C	Contingency Planners						
C	Technology Leaders						
R	Implementation Team						



Key Components of the Framework- 4th Step

Foundation

Ecosystem

Service
Levels

Delivery
Objectives

Preserve
Data

Enable
Recovery

Independently
Test

Requirements: *SDOs must enable the delivery of highest-quality legal services to clients, meet the needs of internal business units, protect and preserves the CIA of assets, and meet ACME's legal, contractual, and ethical obligations.*

Scope: *Entire data set is in scope*

Objective: *RTO/RPO commitment: 4/4 hours.*

Mitigations: ***DMS Vendor Remedy:** 95% = 100% service credit for the period*



ORF – ACME Data Preservation

Foundation

Ecosystem

Service Levels

Delivery Objectives

Preserve Data

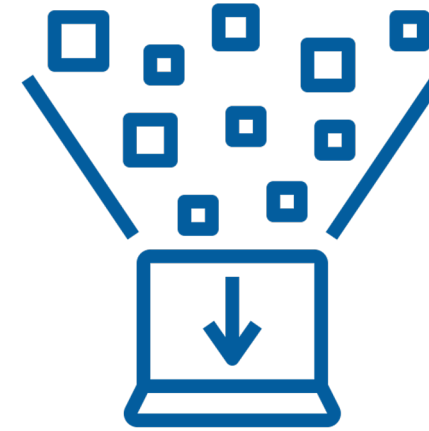
Enable Recovery

Independently Test



Distributed AND Immutable Backups

- Confidentiality
- Integrity
- Availability
- Format, Frequency
- Secure Transfer
- Permanency
- Retention
- Deletion



Operations Critical and Business Critical Data Sets

- User Data
- Business Data
- Processes
- Applications
- Networks
- Systems
- Core Services
- Other



Key Components of the Framework- 5th Step

Foundation

Ecosystem

Service
Levels

Delivery
Objectives

Preserve
Data

Enable
Recovery

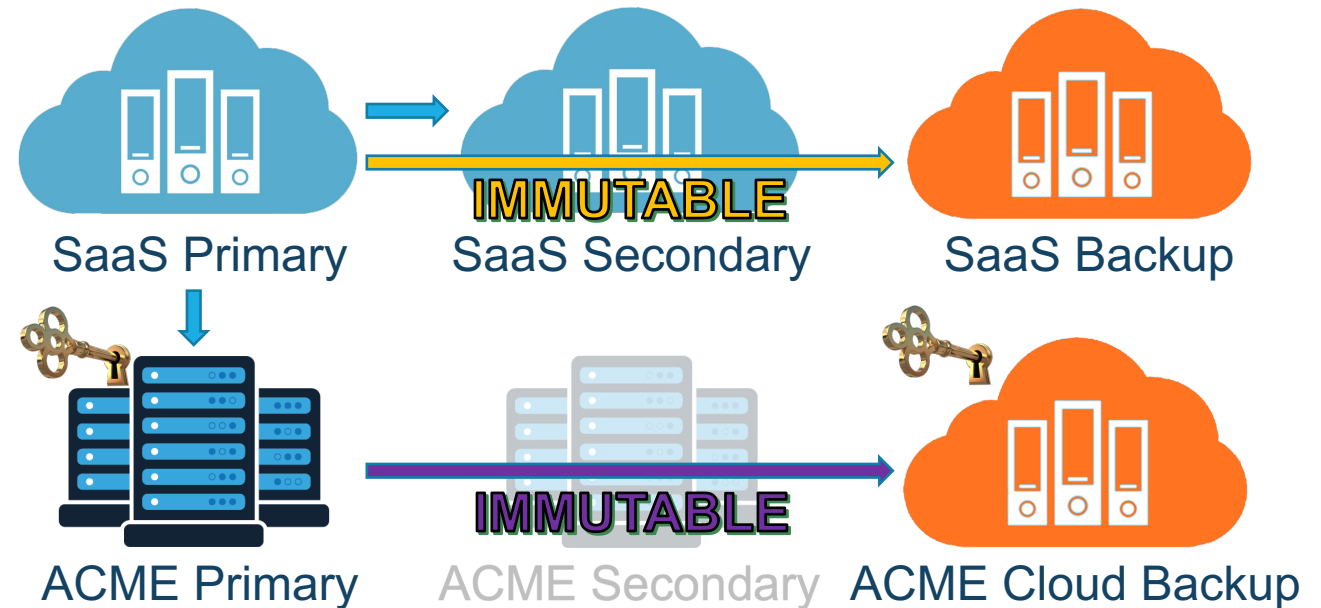
Independently
Test

SaaS Vendor Only:

- Data center replication
- Incremental daily differential writes
- 24-hour commits to a target independent from primary storage
- 90 days of backup

SaaS + Us:

- Auxiliary repository of entire data set
- Select metadata saved to an immutable backup solution in our datacenter
- Replicated to an independent IaaS cloud
- Encryption keys held by ACME
- Daily synchronized and validated incremental backups



Key Components of the Framework- 6th Step

Foundation

Ecosystem

Service Levels

Delivery Objectives

Preserve Data

Enable Recovery

Independently Test



Recovery Environment



Access Redundancy



Update Plans to Include OR



Key Management Policies



Key Components of the Framework- 6th Step

Foundation

Ecosystem

Service Levels

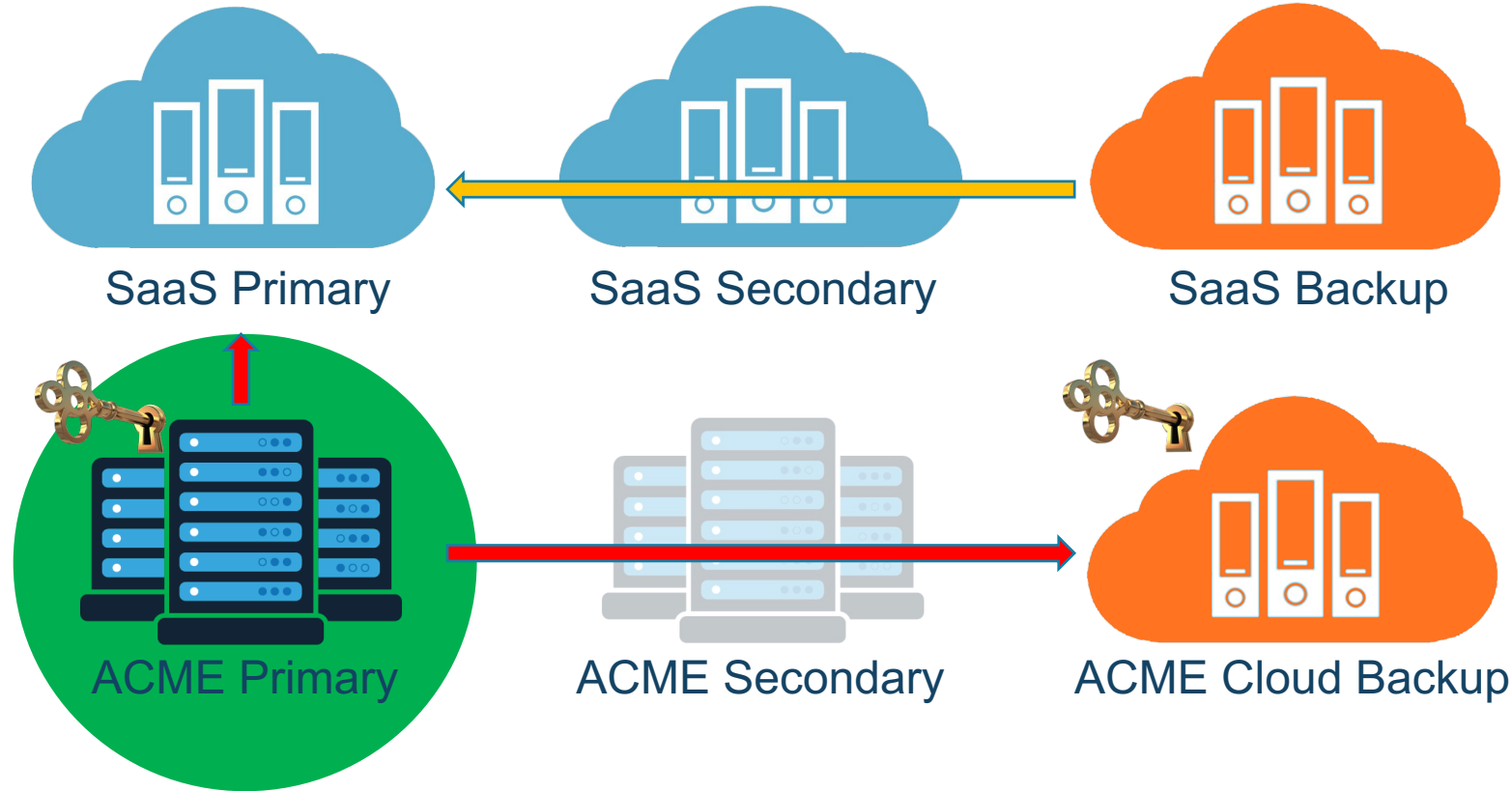
Delivery Objectives

Preserve Data

Enable Recovery

Independently Test

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



Key Components of the Framework- 7th Step

Foundation

Ecosystem

Service Levels

Delivery Objectives

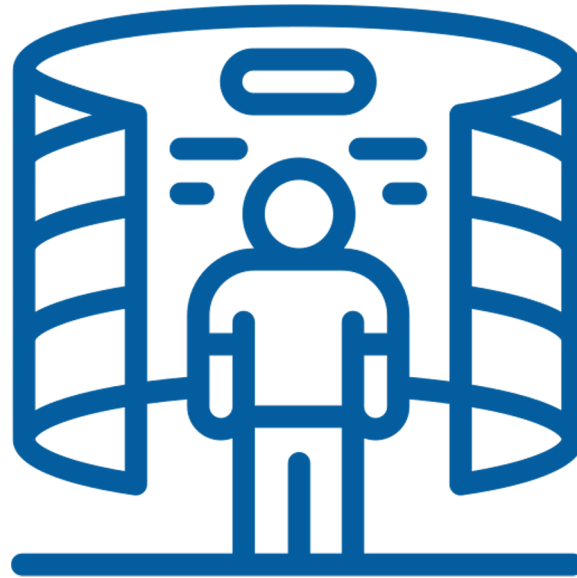
Preserve Data

Enable Recovery

Independently Test



Independent Verification/Validation



Testing, Training, and Exercises



Monitoring and Continuous Improvement



Purpose- To create a guide by which any organization, from any sector and any size can evaluate the maturity of their operational resilience capabilities and provide guidance in how to progress up the Maturity Model

Key Features:

Dual Progression

Designed to Accelerate OR across sectors

Evidence Based Approach

Evaluate at the Rule and Step Level

Evaluate at the Business Unit and Firm Level

	Implementation	Assessment
L0	Identified	Unassessed
L1	Designed	Internally Assessed
L2	Implemented	Independently Assessed
L3	Operating	Audited for Completeness
L4	Integrated*	Audited for Performance

Benefits of the ORF Maturity Model



Clear Operational Resilience Roadmap



Regulatory Alignment and Industry best practices.

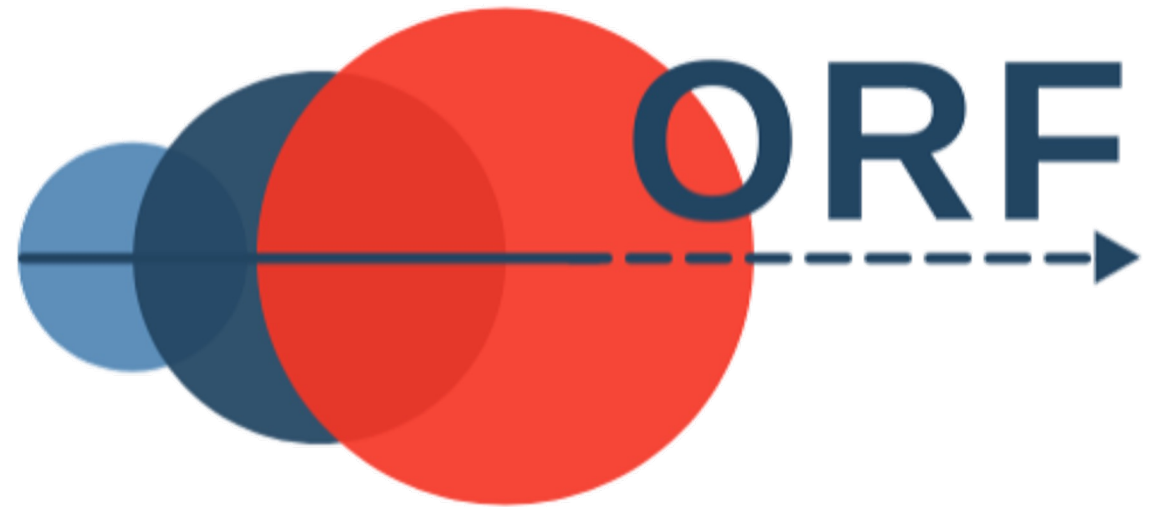


Improved stakeholder confidence and trust.



Operational Risk Mitigation Strategies

- **Disruptive events have never been more common**
- **Resilience is attainable with the ORF as a guide**
- **Organizations wishing to be pioneers of Operational Resilience in their sectors should join GRF communities and get involved**
- **Maturity model will be released next month at our Summit**





Fortify Now So You Can Be Resilient Later!



Download the ORF at www.grf.org/orf



Contact us:

Mark Orsi, CEO, Staff Lead for the ORF - morsi@grf.org

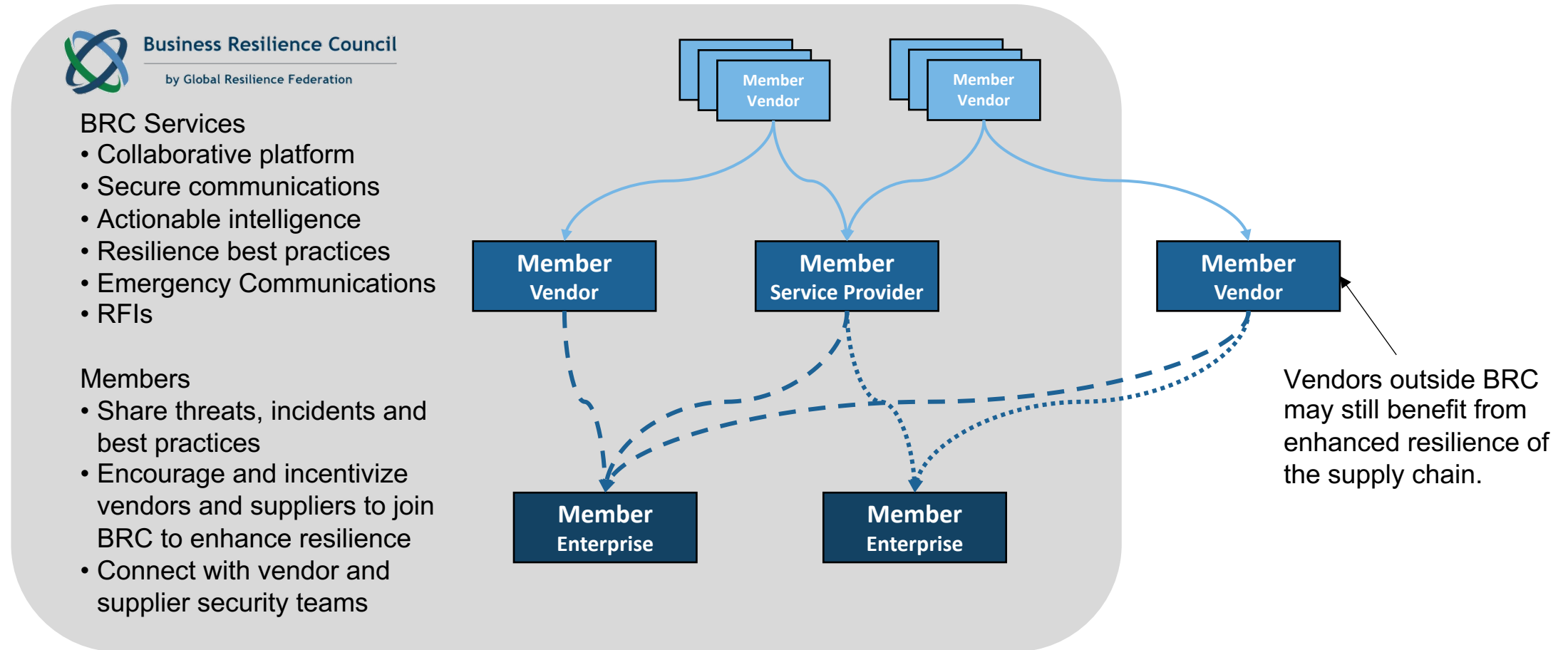


Brian Katula, Project Manager, ORF – bkatula@grf.org



BRC – Third-Party Security Connection (1/2)

The Business Resilience Council (BRC) provides the solution to build connections with the product and security teams of vendors that support your critical business services. When a threat is imminent, or an incident occurs, these connections become vital to your cybersecurity and continuity teams for situational awareness and rapid response. As part of the GRF Network of sharing communities, the BRC has dedicated analysts that provide relevant threats, incidents, vulnerabilities and resilience best practices to your team and to your vendors.



<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/covid-19-implications-for-business>, <https://www.pnas.org/doi/10.1073/pnas.2006991117>
<https://www.whitehouse.gov/cea/written-materials/2021/06/17/why-the-pandemic-has-disrupted-supply-chains/>
<https://kpmg.com/de/en/home/insights/2022/05/the-economic-impact-of-the-russia-ukraine-war.html#:~:text=Due%20to%20the%20start%20of,transportation%20services%20have%20increased%20significantly.>
<https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983>
<https://www.theverge.com/2023/8/5/23821110/hospital-ransomware-attack-us-prospect-medical-cybersecurity-fbi>
https://www.nyc.gov/html/sirr/downloads/pdf/final_report/Ch_1_SandyImpacts_FINAL_singles.pdf
http://stedc.tamucc.edu/files/HARVEY_Update_STEDC_2018Q3.pdf
<https://www.itgovernanceusa.com/blog/lincoln-college-shuts-down-after-157-years-following-ransomware-attack>
<https://www.beckershospitalreview.com/cybersecurity/ransomware-shuts-down-facilities-at-connecticut-health-system.html#:~:text=A%20cyberattack%20at%20Manchester%2Dbased,diversions%2C%20NBC%20Connecticut%20reported%20Aug.>
<https://www.cbsnews.com/news/prospect-medical-cyberattack-california-pennsylvania-hospital/>
<https://comptroller.texas.gov/economy/fiscal-notes/2021/oct/winter-storm-impact.php#:~:text=Although%20Winter%20Storm%20Uri's%20devastation,damage%20and%20forgone%20economic%20opportunities.>
<https://data.austintexas.gov/stories/s/Year-in-Review-Winter-Storm-Uri/hpvi-b8ze/>
<https://afb.accuweather.com/blog/the-economic-impact-of-hurricanes-on-your-business>
<https://www.womply.com/impact-of-severe-weather/hurricanes/>
<https://www.clickondetroit.com/all-about-ann-arbor/2023/08/29/university-of-michigan-shuts-down-internet-due-to-security-concern/>

All Icons: : Flaticon.com

Critical icons created by Icon.verse - Flaticon
Inventory icons created by IconBaandar - Flaticon
Ecosystem icons created by Eucalyp - Flaticon
Automation icons created by Uniconlabs - Flaticon
Leadership icons created by Uniconlabs - Flaticon
Classification icons created by Iconjam - Flaticon
Ecosystem icons created by Eucalyp - Flaticon
Computer icons created by Uniconlabs - Flaticon
Target icons created by Eucalyp - Flaticon
Client icons created by Freepik - Flaticon
Process icons created by Uniconlabs - Flaticon
Weak icons created by Freepik - Flaticon
Minimum icons created by rcherem - Flaticon
Dependency icons created by juicy_fish - Flaticon
Sla icons created by Freepik - Flaticon
Restore icons created by surang - Flaticon
Security icons created by srip - Flaticon
Big data icons created by Parzival' 1997 - Flaticon
Data recovery icons created by Smashicons - Flaticon
Access icons created by Eucalyp - Flaticon
Subscription icons created by Freepik - Flaticon
Solution icons created by Uniconlabs - Flaticon
Stamp icons created by Freepik - Flaticon
Monitoring icons created by Freepik - Flaticon
Simulation icons created by Freepik - Flaticon



Annex



Disruption:

- Outage Occurred in 2017
- Caused by a typo during a debugging session
- Lead to more servers being taken offline than intended
- Outage Cascaded through several subsystems
- High Error Rates lead to a mass outage

Service:

- Primarily affected ACME D4 object storage cloud platform
- Used by many to store and retrieve data
- Primary use case static website content, images, backups, and application data



Customers:

- 10s of thousands to 100s of thousands were impacted
- Large Enterprises and Corporations:
 - Potential Harm: High
 - Potential Vulnerability: Low
- Government Agencies and Emergency Services:
 - Potential Harm: High
 - Potential Vulnerability: Medium
- E-commerce Platforms and Retailers:
 - Potential Harm: High
 - Potential Vulnerability: Medium
- Media and Streaming Services:
 - Potential Harm: Medium
 - Potential Vulnerability: Low

Response/Impact:

Impact:

- Website and Application Downtime
- Data Access Disruptions
- Financial Losses
- User Frustration and Trust Erosion
- Operational Disruptions
- Reputational Damage

Response:

- Identification of Root Cause
- Communication with Customers
- Restoration Efforts
- Mitigation Measures



Challenges faced:

- Identifying the specific cause of the issue promptly.
- Communicating effectively with a large and diverse customer base.
- Balancing the need to restore service quickly while ensuring the root cause was fully addressed.

Lessons Learned

- The importance of thorough testing and safeguards to prevent human errors.
- Enhancing communication channels to provide timely updates to customers.
- The need for improved system-level protections to prevent similar cascading failures.

Impaired Service Delivery:

- Offering read-only access to D4 for retrieving data, even if write operations were disabled.
- May only be select data for high priority customers
- Prioritizing the recovery of critical customer data and services, such as data needed for emergency services or essential infrastructure.

Customer Prioritization:

- Balance Customer Vulnerability with Potential Systemic Harm with other priorities such as financial relevance to the firm
- Giving priority to customers with mission-critical applications, such as healthcare providers or emergency services.
- Offering dedicated support and assistance to customers facing significant financial losses or public safety concerns.

