



Business Resilience Council

by Global Resilience Federation

*Software and Supply Chain Assurance Forum*

# “Strategy for Cyber-Physical Resilience”

*President’s Council of Advisors for Science & Technology (PCAST)*

## Operational Resilience Framework

Sept 17, 2024, MITRE HQ, McLean, VA



# Operational Resilience Framework

## Addressing Minimal Viable Services During and After a Critical Event



**Moderator**  
Charlie Tupitza  
Dr Community Development  
Global Resilience Federation



Mark Orsi  
CEO  
Global Resilience Federation



Kevin Frost  
Chief Product Officer  
Fusion3 Consulting

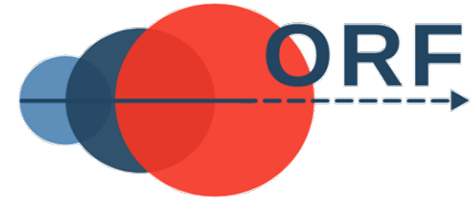


# We Are All Ears



Business Resilience Council

by Global Resilience Federation



We are here to share  
and take advantage  
of your feedback.



# History of the Operational Resilience Framework

Who developed the ORF?

ORF as referenced in the **PCAST “Strategy for Cyber-Physical Resilience”**

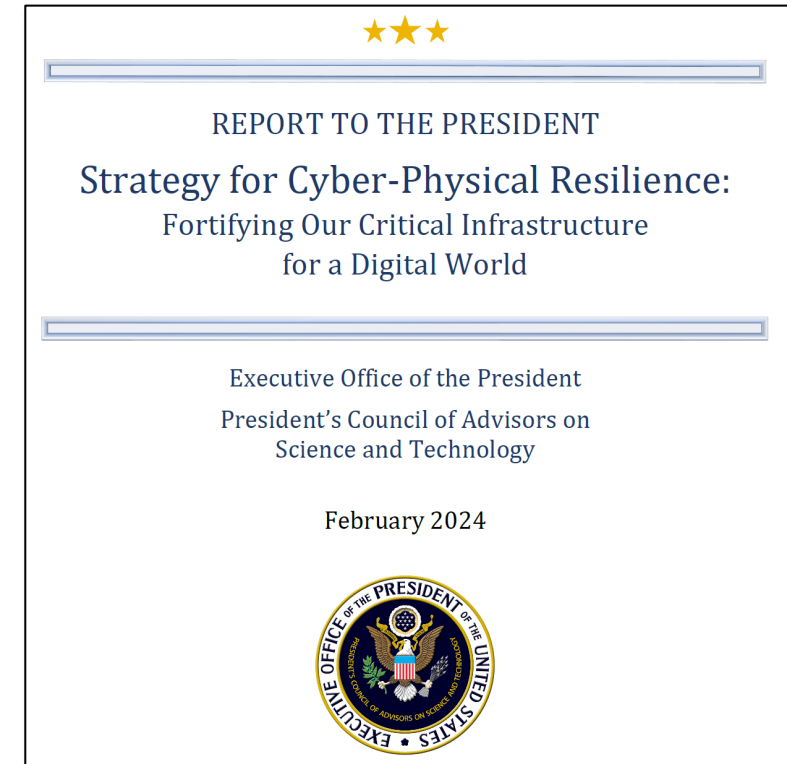
What is a minimal viable service?

# PCAST Strategy for Cyber-Physical Resilience

**Resilience**, ability of a system to anticipate, withstand, recover from, and adapt to cyberattacks and natural or accidental disruptions.<sup>1</sup>

**Working Group Co-Leads:** Phil Venables from Google Cloud  
Eric Horvitz the Chief Scientific Officer for Microsoft.

A diverse group of 100 additional experts and stakeholders consulted.



[whitehouse.gov/wp-content/uploads/2024/02/PCAST\\_Cyber-Physical-Resilience-Report\\_Feb2024.pdf](https://whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf)

<sup>1</sup> Ross et al. (2021 December). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Vol. 2, Rev. 1.



## Primary Elements:

- Seven Step Path
- 36 High-level Rules
- Maturity Model
- Implementation Aids
- Exercises and Scenarios
- Glossary

Reduce operational risk, minimize service disruptions and limit systemic impacts from destructive attacks and adverse events

---

### ORF Development Team – 100+ Companies and Regulators

Trey Maust, Executive Chair  
**Lewis & Clark Bank**

Susan Rogers, Executive Dir  
**SMBC**

Charles Blauner, CISO  
**Team8**

Jon Washburn, CISO  
**Stoel Rives LLP**

Alex Sharpe, Principal  
**Sharpe Management**

Judy Erbs, VP  
**Mastercard**

George Shea, Chief Technologist  
**Foundation for Defense Democracies**

Bob Blakley, Partner  
**Team8**

Jennifer Buckner, SVP  
**Mastercard**

Judy Erbs, VP  
**Mastercard**

Simon Chard, Director  
**S&P Global**

John DiNuzzo, AVP  
**Metlife**

Bill Nelson, Chairman  
**GRF**

John Brennan, Manager  
**American Express**

Mark Orsi, President/CEO  
**GRF**

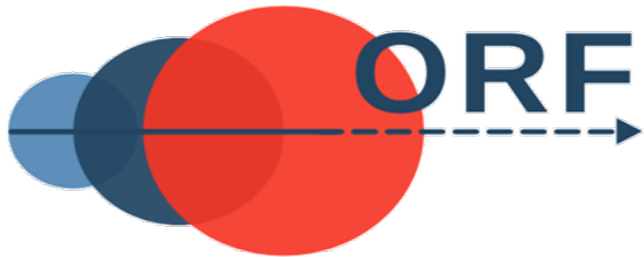
Chris Denning, CSO  
**GRF**

Barry Richards, Executive Dir  
**GRF**

Staci Elliott, Analyst  
**GRF**

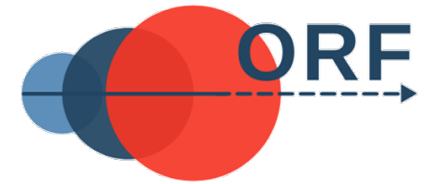
Brian Katula, Project Manager  
**GRF**





## Key Principals:

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



What have we learned about the framework?

How can an organization take advantage of it?

Is it just another pile of controls to stack on the existing burden of risk managers?

# Taking Advantage of Informed References



The ORF incorporates and compliments existing standards and frameworks such as CIS, CSF, NIST 800-53 & 171, ITIL and ISO 27001 for cyber and physical security.

## **Confidentiality, Integrity & Availability (CIA) Triad:**

We have observed a cultural shift from Confidentiality and Integrity **to include Availability** of information and services when and after an incident occurs.



# Taking Advantage of the ORF Maturity Model to Communicate

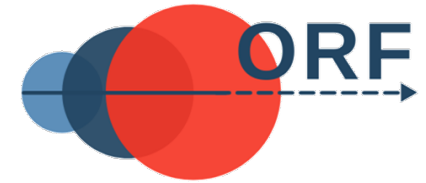


**Purpose** –To create a guide by which any organization can evaluate the maturity of their operational resilience capabilities and provide guidance on how to improve.

## Key Features:

- Separates Assessment and Implementation Level
- Applicable to organizations of all sizes
- Evidence Based Approach
- Evaluate at the Rule and Step Level
- Clear roadmap to enhance operational resilience
- Better understanding of risk exposure
- Alignment industry best practices
- Improved stakeholder confidence and trust





## Half Day Tabletop Exercises Highlighting the value of the Operational Resilience Framework



# Tabletop Exercise: Disruption of ACH Critical Functions



Business Resilience Council

by Global Resilience Federation



**NACHA**  
The Electronic Payments Association®



**700 financial institution representatives participated in tabletop exercise** simulating a disruption in ACH Critical Functions, and separate Cross-Sector exercise to show the value of the Framework.

Partnered with **Nacha** who **governs the ACH Network**, the payment system that drives Direct Deposits and Direct Payments with the capability to reach all U.S. bank and credit union accounts.

**After Action Report available:** [ctupitza@grf.org](mailto:ctupitza@grf.org)



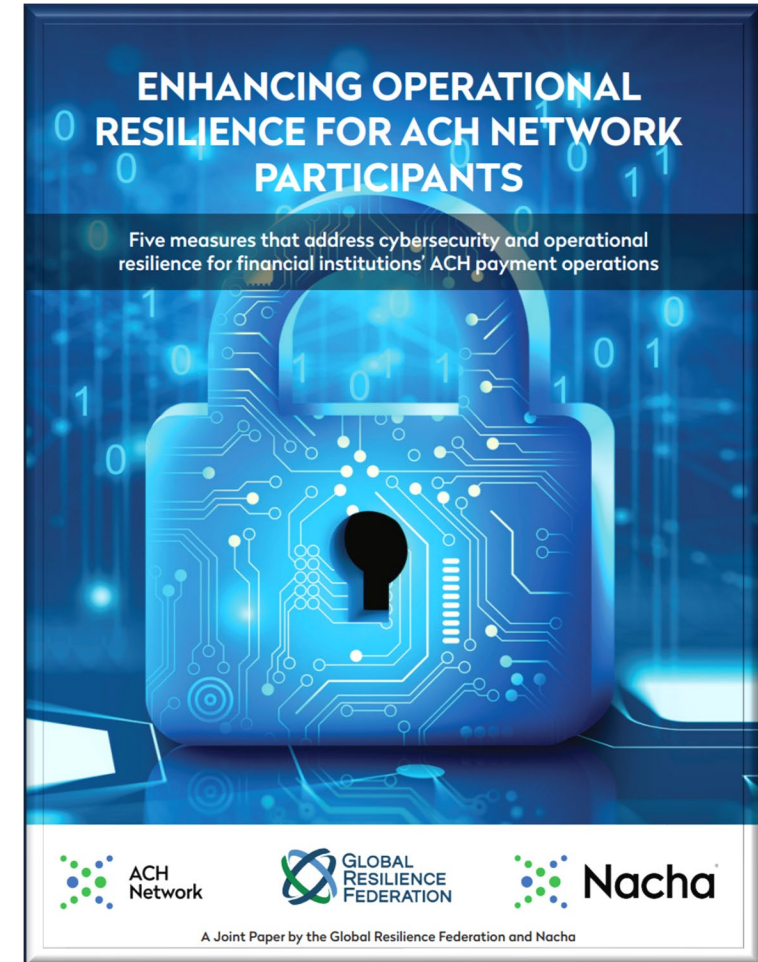
# GRF and Nacha Joint Paper

## GRF and Nacha Joint Paper

### Enhancing Operational Resilience for ACH Network Participants

#### Measures for consideration:

1. Develop, review, and update annually all ACH incident and recovery plans that address disruption or impairment to ACH Critical Services.
2. Define minimum ACH service levels that can satisfy the needs of customers, partners and counterparties before the service is no longer useful.
3. Establish Service Delivery Objectives for how quickly ACH services can be restored to a target impaired state with considerations of both business and technical dependencies.
4. Implement recovery environment, processes, and mechanisms to meet Service Delivery Objectives for ACH services.
5. Independently evaluate and test ACH service restoration processes against Service Delivery Objectives



# Exercise Structure



Designed for large groups to test operational resilience capabilities in the face of extreme disruptions

- Developed by Member Driven ORF Working Group
- Virtual Tabletop Half-Day Exercise held on two days
- Directed by Bill Nelson, GRF Chair

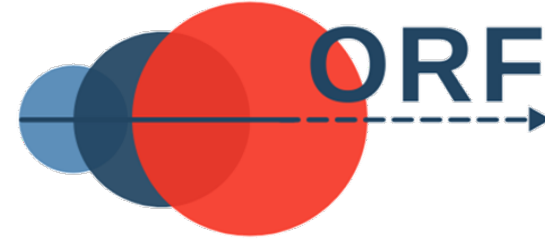
**Panelists** – Provided expertise pertaining to the scenario and each inject, responded to data from participants to provide perspective

- Trey Maust - Lewis & Clark Bank
- Bob Blakely - Team8
- Mark Harvey - Regeneron Pharmaceuticals
- Michael Herd, Devon Marsh, Jordan Bennett, Amy Morris - Nacha

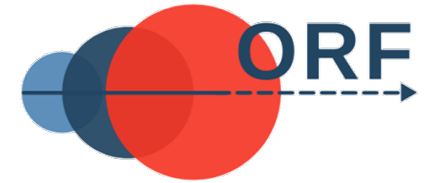


# Key Takeaways Summary

1. Operational resilience maturity and challenges
2. Operational Resilience in the face of uncertainty
3. Decision making for resilience
4. Minimization of systemic impacts
5. Communications to regulators, public, vendors, and customers
6. Fighting disinformation
7. Ability to handle a secondary attack
- 8. Resilience in scenarios where third-parties are unable or unwilling to render aid**
9. Trust in financial institutions



# Regulations



We have been in conversations with regulators, the White House, and at the C level across sectors.

Some fear regulatory action, does this have merit?



# *Move on from only Focusing on Cyber Resiliency*



*What else is affecting overall Resiliency; other than hacking, ransomware, and bad code pushes?*

*Where are some of the Supply Chain blind spots?*

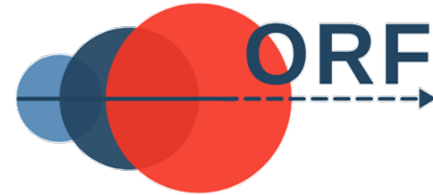


# How to Take Advantage of the Framework



Business Resilience Council

by Global Resilience Federation



## Participate in Resilience focused Activities:

- Task Force Continual Improvement
- White Papers
- Sharing Lessons Learned and Best Practices
- Attend Virtual and In-person Exercises
- Annual Risk Summit at the Dolphin Inn in Florida, November

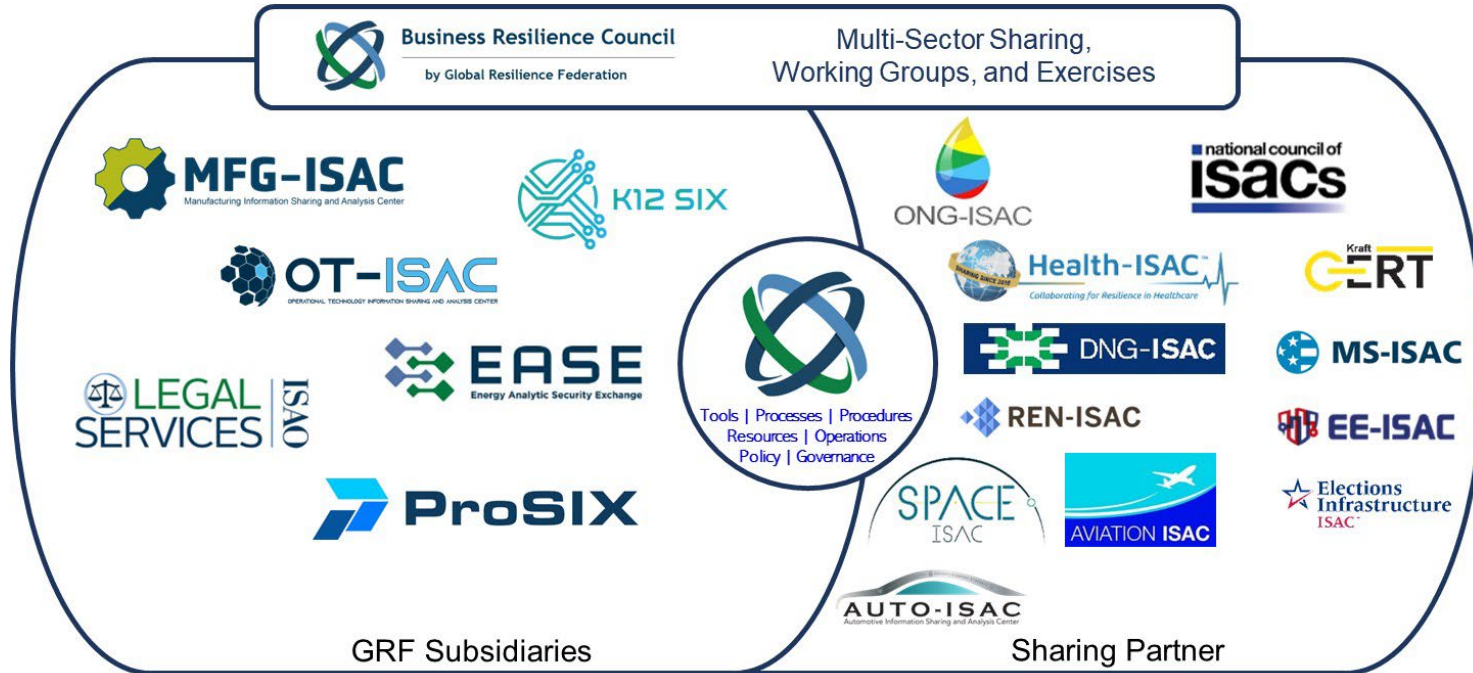
Contact us: [ctupitza@grf.org](mailto:ctupitza@grf.org)

© 2024 Global Resilience Federation, Inc.



# Business Resilience Council (BRC)

## Reducing Risk Through Collective Defense



The Business Resilience Council (BRC), part of the Global Resilience Federation, is a multi-sector, collaborative defense community.

Members share insights on a spectrum of Cyber to Geopolitical threats.

In-depth reports, ad-hoc meetings, community calls, and secure messaging provide members with the intelligence needed to address emerging risks.



# About the Speakers



## Business Resilience Council

by Global Resilience Federation

**Mark Orsi**  
morsi@grf.org

CEO of the Global Resilience Federation, 'an expert consulted' for the PCAST report. The GRF's Business Resilience Council is responsible for creating and continual improvement of the Operational Resilience Framework.

**Kevin Frost**  
kevin@fusion3consulting.com

Well-known and respected leader in business continuity and integrated risk management as the Chief Product Officer at Fusion3 Consulting, a small business, leading the risk efforts externally for a Global Consulting company with over 45,000 employees and others. Kevin is developing a ServiceNow accelerator for the ORF.

**Charlie Tupitza**  
ctupitza@grf.org

Former US Head of Cyber Resilience, AXELOS (ITIL),  
Charter Member of PPD-21 Cyber Security for Critical Infrastructures working group.  
Former Cyber and Data Protection Lead for Americas Small Business Development Centers  
Member Critical Infrastructure Cybersecurity Forum ten years  
Active Participant in this Software and Supply Chain Assurance Forum, ten years



# What is the Business Resilience Council?

**Information Sharing:  
Cyber, Physical, Geopolitics,  
Unrest, Best Practices**

**Playbooks, Exercises,  
Working Groups**

**Operational  
Resilience**

## **Business Resilience Council**

---

**by Global Resilience Federation**

<https://www.grfbrc.org/>

**Cross-Sector  
Collaboration**

**Artificial Intelligence  
Security & Trust**

**Third-Party  
Risk**

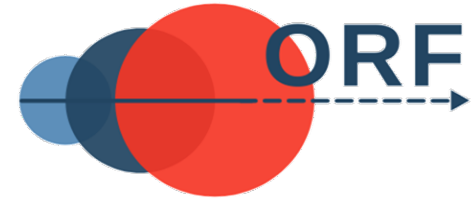


# We Are All Ears



Business Resilience Council

by Global Resilience Federation



Questions?  
Thoughts?

