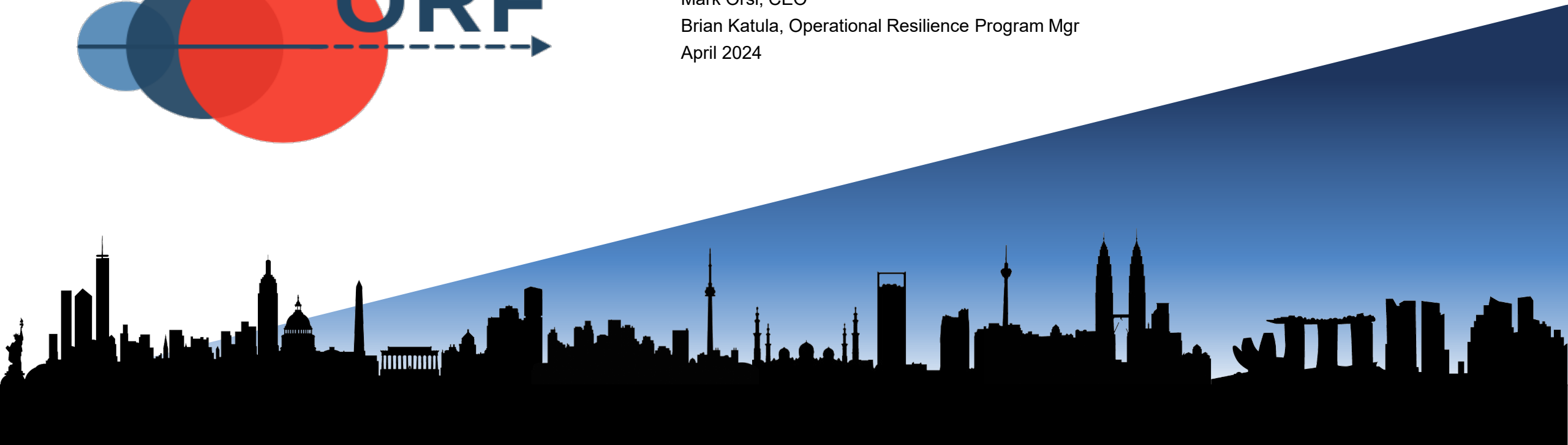
Business Resilience Council

by Global Resilience Federation

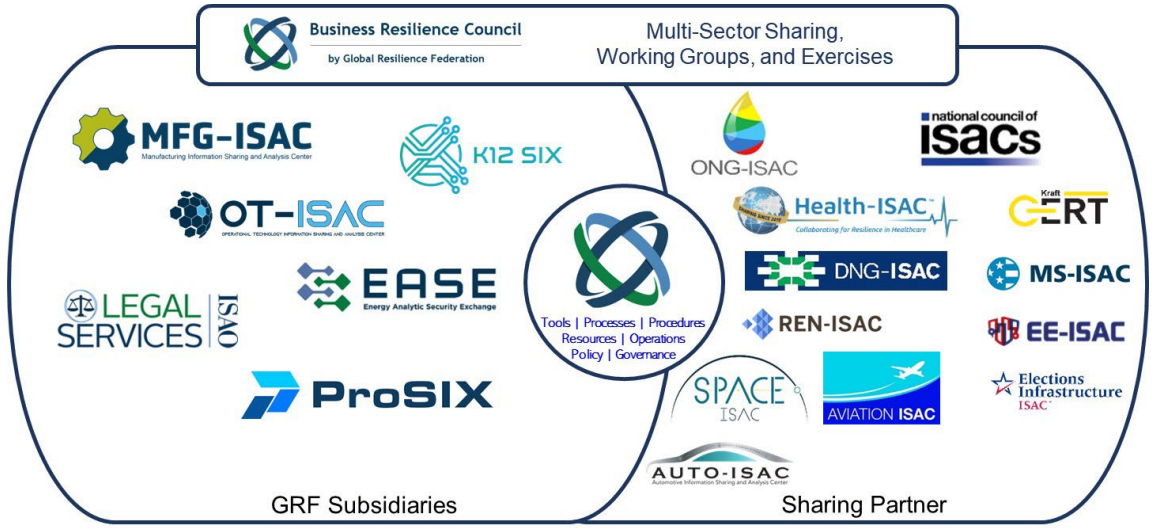
Strengthening Collective Resilience

ORF

Mark Orsi, CEO
Brian Katula, Operational Resilience Program Mgr
April 2024



Business Resilience Council (BRC)



Reducing Risk Through Collective Defense

The Business Resilience Council (BRC), part of the Global Resilience Federation, is a non-profit, multi-sector, collaborative defense community where members share insights on a spectrum of threats – from Cyber to Geopolitical. BRC Services – ranging from in-depth reports and ad-hoc meetings to community calls and secure messaging – equip members with intelligence needed to address emerging risks.

By joining, you tap into a networked ecosystem of defense, enhancing your firm's resilience through shared knowledge and collective action.

TLP: CLEAR

What is the Business Resilience Council?

Playbooks, Exercises, Working Groups

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

Operational Resilience

Business Resilience Council

by Global Resilience Federation

Visit us at: https://www.grfbrc.org/

Cross-Sector Collaboration

Artificial Intelligence Security & Trust

Third-Party Risk

TLP: CLEAR

What is Operational Resilience?

Operational resilience is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.

Source: Sound Practices to Strengthen Operational Resilience
October 2020 Interagency Paper from the Federal Reserve Board, FDIC, and OCC:

TLP: CLEAR

Operational Resilience Framework (ORF)

Operational Resilience Framework – Mission

To reduce operational risk, minimize service disruptions and limit systemic impacts from destructive attacks and adverse events.

https://www.grfbrc.org/orf

ORF Team – 100+ Companies and US Financial Regulators

Trey Maust, Executive Chairman, Lewis & Clark Bank
David LaFalce, SVP, Wells Fargo
Charles Blauner, CISO, Team8
John DiNuzzo, AVP, Metlife
John Brennan, Manager, American Express
Bill Nelson, Chairman, GRF
Mark Orsi, President and CEO, GRF
Jordan Bennett, Sr Director, Nacha
Chris Denning, CSO, GRF
Brian Katula, TPM, GRF
Jon Washburn, CISO, Stoel Rives LLP
Alex Sharpe, Principal, Sharpe Consulting
John Carlson, VP Resilience, American Bankers Assoc
Dr. Georgianna Shea, Chief Technologist, FDD
Devon Marsh, Sr Director, Nacha
Jennifer Buckner, SVP, Mastercard
Judy Erbs, VP, Mastercard
Susan Rogers, Executive Director, SMBC
Gina Gavito, VP Global Crisis Mgmt, Capital Group
Spruille Braden, Global Head ERP, Citi
Bob Blakley, Operating Partner, Team8

Reviewers include 100+ Companies and US Financial Regulators (OCC, FRB, FDIC)

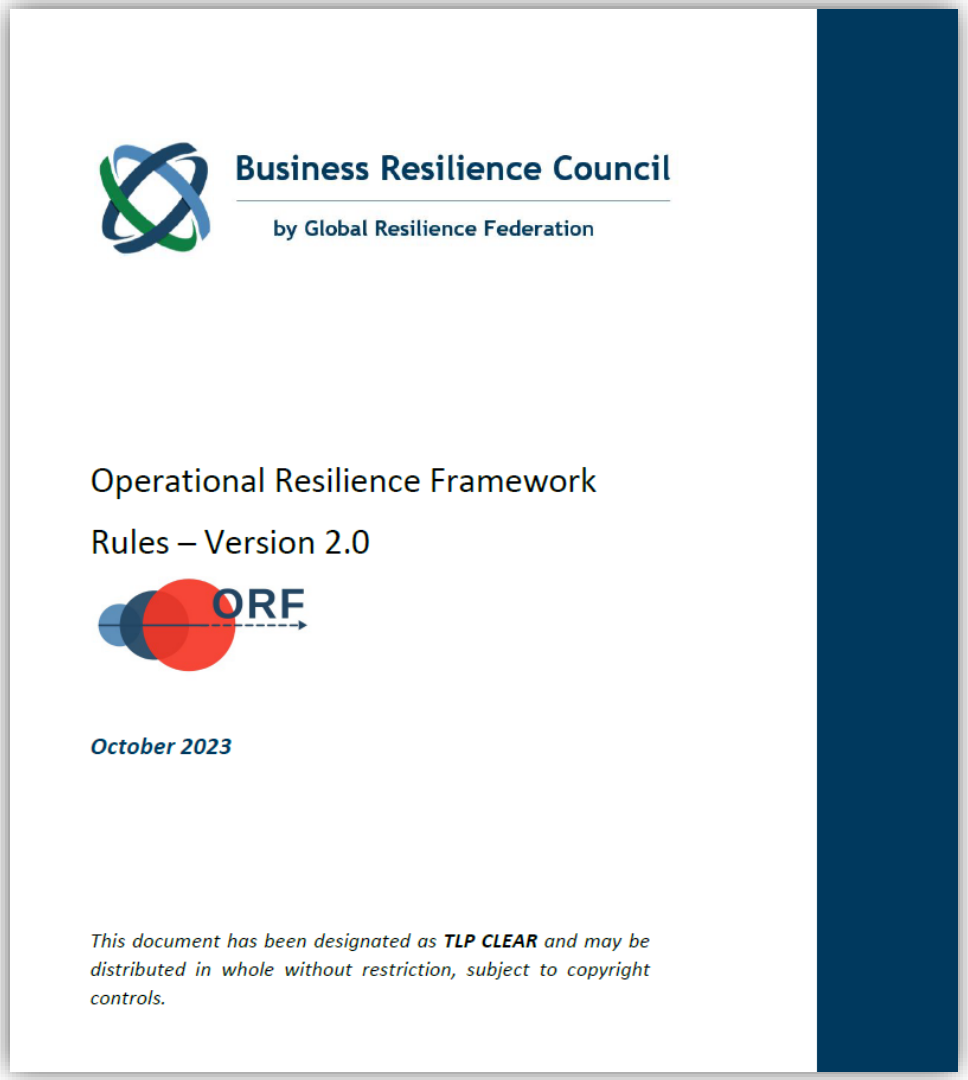
TLP: CLEAR

ORF Primary Elements

https://www.grfbrc.org/orf

Primary Elements:

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



TLP: CLEAR

ORF Path to Operational Resilience

https://www.grfbrc.org/orf

1. **Build the Foundation:** Implement an industry-recognized IT and Cybersecurity control framework.
2. **Ecosystem:** Understand the organization's role in the ecosystem.
3. **Service Levels:** Define the Minimum Viable Service Levels for each Operations Critical and Business Critical service.
4. **Delivery Objectives:** Establish Service Delivery Objectives for each Operations Critical and Business Critical service.
5. **Preserve Data:** Preserve the Data Sets necessary to support Operations Critical and Business Critical services.
6. **Enable Recovery:** Implement processes to enable recovery and restoration of Operations Critical and Business Critical services to meet Service Delivery Objectives.
7. **Independently Test:** Independently evaluate design and test periodically.

ORF Key Principals

https://www.grfbrc.org/orf

Key Principals:

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

TLP: CLEAR

ORF Key Terms

https://www.grfbrc.org/orf

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

Minimum Viable Service Level – The lowest possible level of service delivery where the service is still usable and valuable to customers and counterparties.

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.

Business Critical – Business critical components are data, systems and processes required to prevent sustained disruption of business services required for the organization's continuity.

All Other Services (AOS) – Services necessary to support the business at pre-event levels.

Operations Critical and Business Critical Data Sets – Immutable and distributed backups of data sets for recovery and restoration of critical services including:

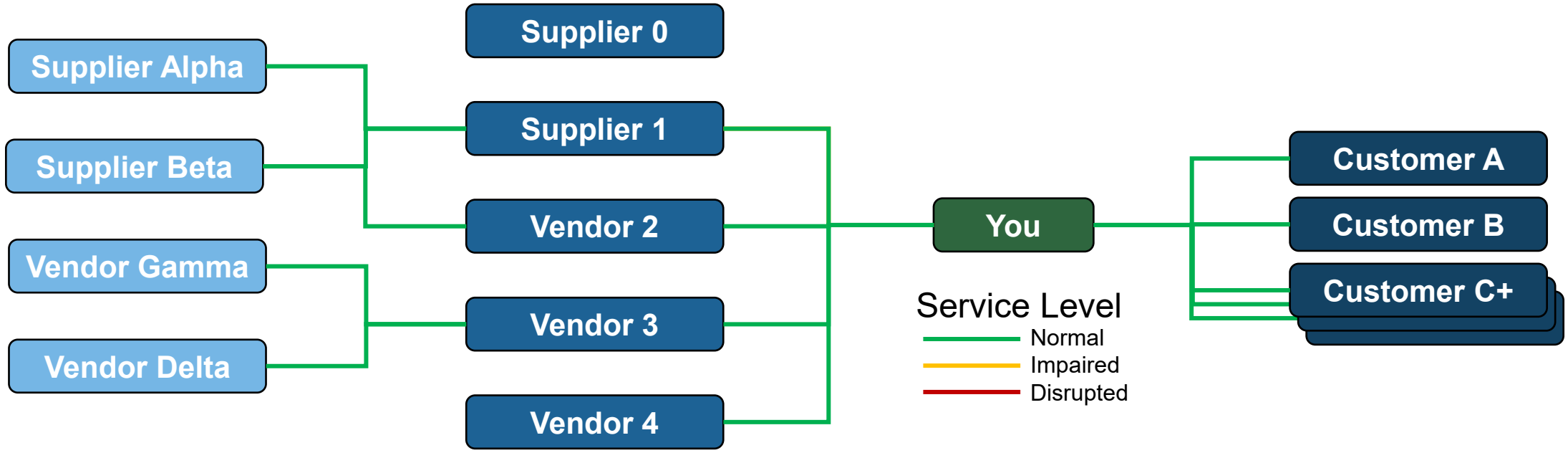
- User Data
- Business Data
- Processes
- Applications
- Networks
- Systems
- Active Directory
- Other

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

Data Restoration Objectives – The objectives that define the specific data that must be restored to reach the impaired level of operationality set by the Operations Recovery 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.

This is your supply chain…

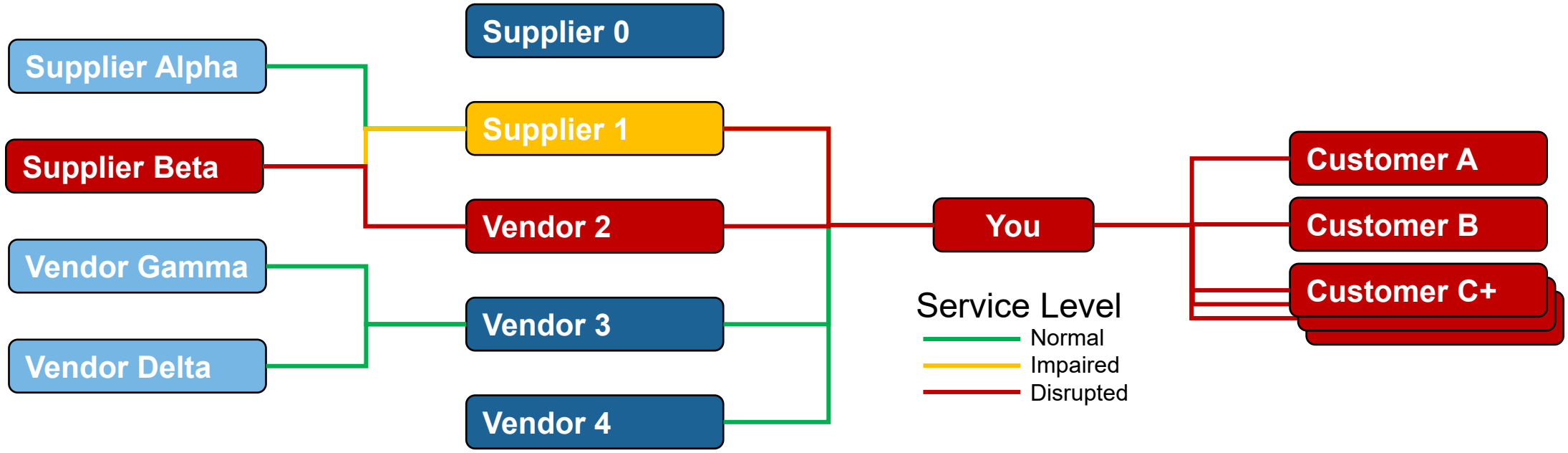


Each box represents a distinct organization, and each line is a service they provide

Many of our critical vendors can bring our services to a screeching halt

And many of them depend on common vendors with little to no visibility

With operational disruptions …



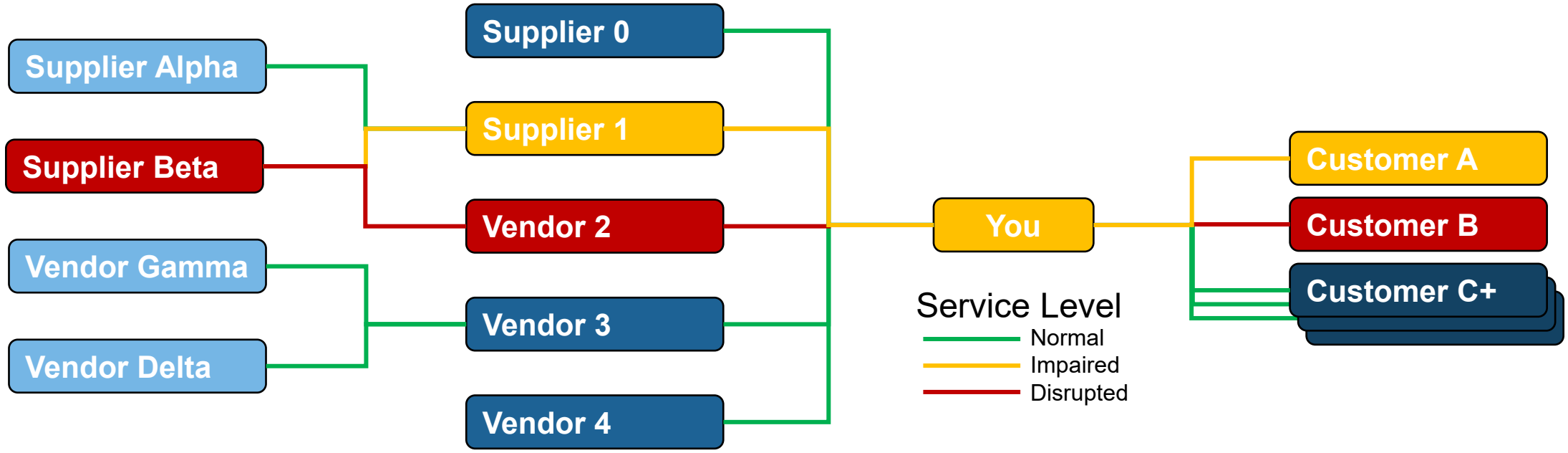
Green Services are running at 100%, Yellow are impaired, Red are 100% disrupted

Without Operational Resilience, any Vendor disruption may significantly impact Customers

Whether it is a third, fourth, or nth party, Critical disruptions can take your service offline

TLP: CLEAR

Now with Operational Resilience



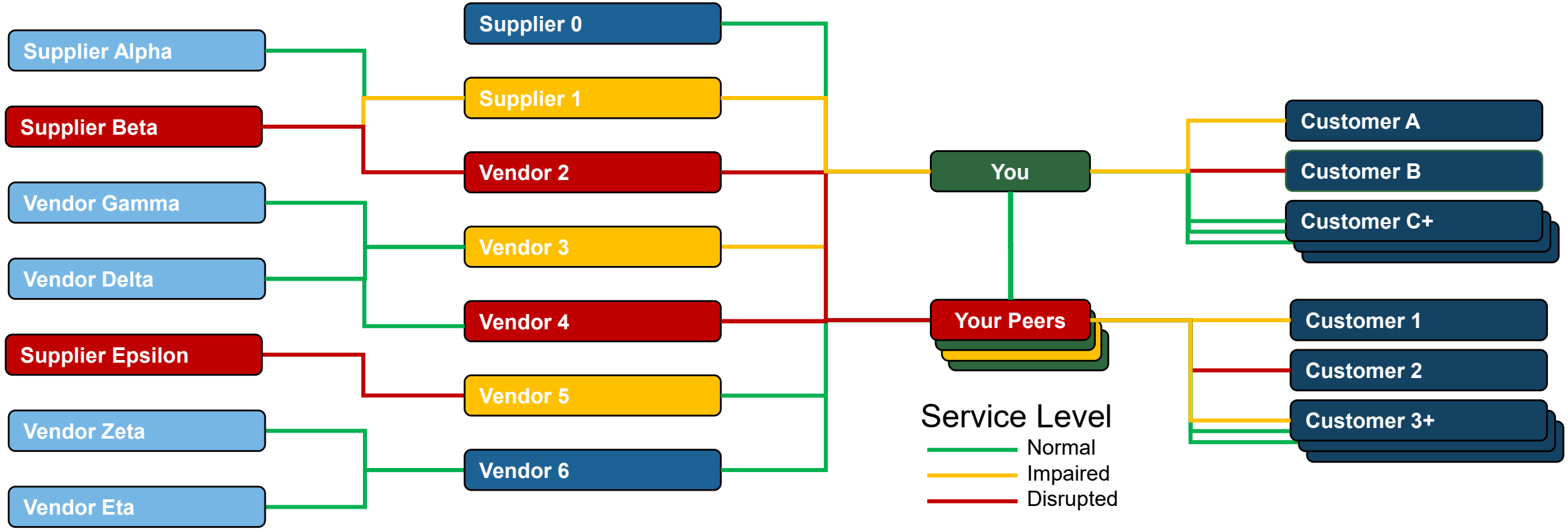
Yellow Lines are Services that are delivered at or above the Minimum Viable Service Level

With Operational Resilience Principals baked into your supply chain, many service failures can be endured and Systemic Impacts minimized

Risks can be significantly reduced and can be mapped to specific business outcomes to align all parties

TLP: CLEAR

Operational Resilience for the Industry



The Benefits only get more pronounced as the principals of Operational Resilience are applied across industries

Just like your own vendors, many of your peers depend on common critical vendors with little to no visibility

Systemic impact must be minimized and there is a straightforward path to achieving this

TLP: CLEAR

Enhancing Resilience – We need our Third Parties

Security and Resilience Best Practices

Collective Defense

Continuous Improvement and Collaboration

Proactive Communication

Engaging Third Parties for Enhanced Resilience

Recognition for superior service

Compliance with customer requirements

Clear, Trusted Lines of Communication

A Network of Likeminded Organizations

Next Steps

Identifying Security and Resilience Practitioners

Identify Minimum Viable Service Levels

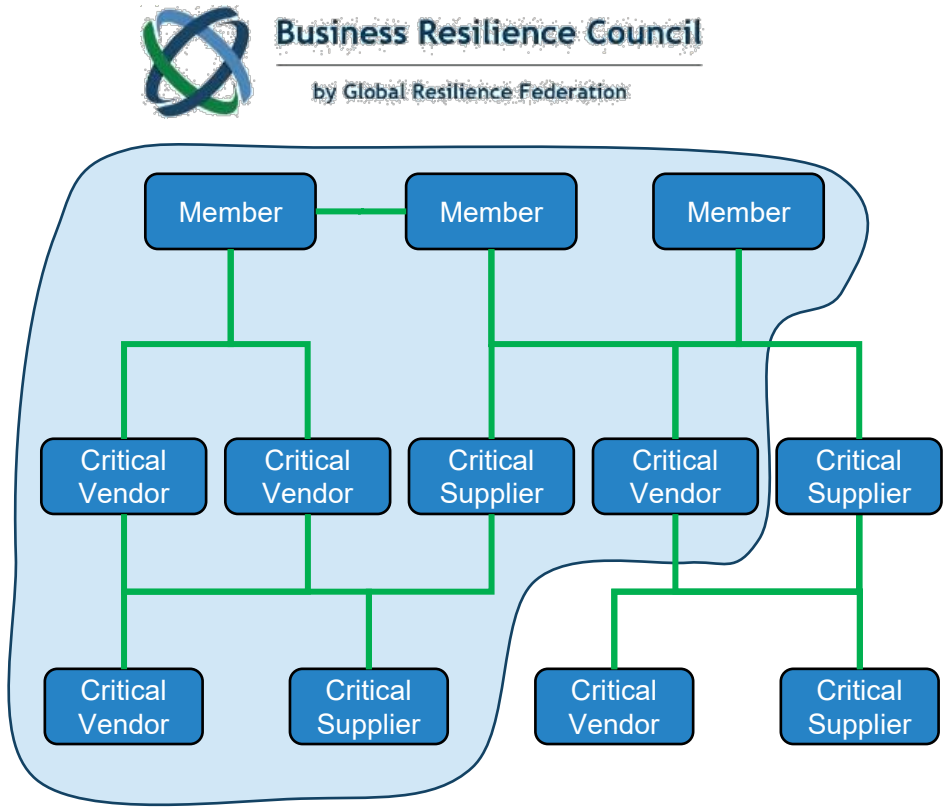
Collective Defense Communities

Updates To Agreements

Third-Party Risk Connection

The Business Resilience Council (BRC) of the Global Resilience Federation (GRF) facilitates essential connections between product and security teams of vendors and suppliers crucial to business services. In the face of immediate threats or incidents, these links are crucial for cybersecurity and continuity teams to maintain situational awareness and to execute swift responses. As a component of the GRF's network of sharing communities, BRC's specialized analysts deliver pertinent information on threats, incidents, vulnerabilities, and resilience best practices to its members, encompassing asset owners, operators, vendors, suppliers, partners, and various third-parties.

BRC Products and Services	RISK
Monthly and Semi-Annual Reports	☑
Ad-Hoc Meetings on Emerging Threats	☑
Monthly Community Calls	☑
Sharing Best Practices	☑
Peer Working Groups	☑
Secure Community Messaging / Chat	☑



Enhance Resilience in Four Steps

1. Join BRC as a TPR member
2. Connect and communicate directly with vendor security teams.
3. Encourage and incentivize your vendors to join during assessments and procurement.
4. Collaborate to enhance collective defense, security, and resilience.

TLP: CLEAR

Enhancing Resilience – Remaining Questions

How do we use the collective voice to drive change?

How do we get the message to mid-sized vendors?

How do we communicate with member organizations?

BRC – Risk Team Membership

The Business Resilience Council's Risk Team Membership informs third-party risk, supply chain risk, risk management, and compliance teams about emerging threats, major incidents, and systemic risks, and facilitates collaboration with peers to address these threats, respond quickly and collectively to vendor incidents, and share best practices to reduce risk for your firm.

All-Hazards Reports

- Third Party and Supply Chain Risk
- Cyber, Physical, Geopolitical, Business Resilience, Systemic
- Topical: Ransomware, Russia/Ukraine, China/Taiwan, Supply Chain, Pandemic, Climate/Major weather, Physical Attacks, Sanctions, New Regulations/Policies, etc.

Working Groups

- Third-Party and Supply Chain Incident Response
- Operational Resilience
- AI Governance

Community Calls

- Monthly Risk and Resilience Calls
- Ad-hoc calls on emerging threats, vendor incidents, regional issues

Call to Action

Help us build security and resilience for your organization and the sector:

- Inform your security and resilience teams about the free Operational Resilience Framework and exercises
- Connect us with your teams to collectively encourage critical vendors and suppliers to contribute to collaborative defense
- Join the BRC and help us refine the program to provide value and reduce risk for your firm

https://www.grfbrc.org/

https://www.grfbrc.org/riskteam

Build an ecosystem of security and resilience to include third parties