GRC SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by **MetricStream**

Power What's Next

Operational Resilience

Agenda

- Current Market Situation
- Operational Resilience Overview
- Acts and Regulations
- How to be Resilient?
- MetricStream Product Overview

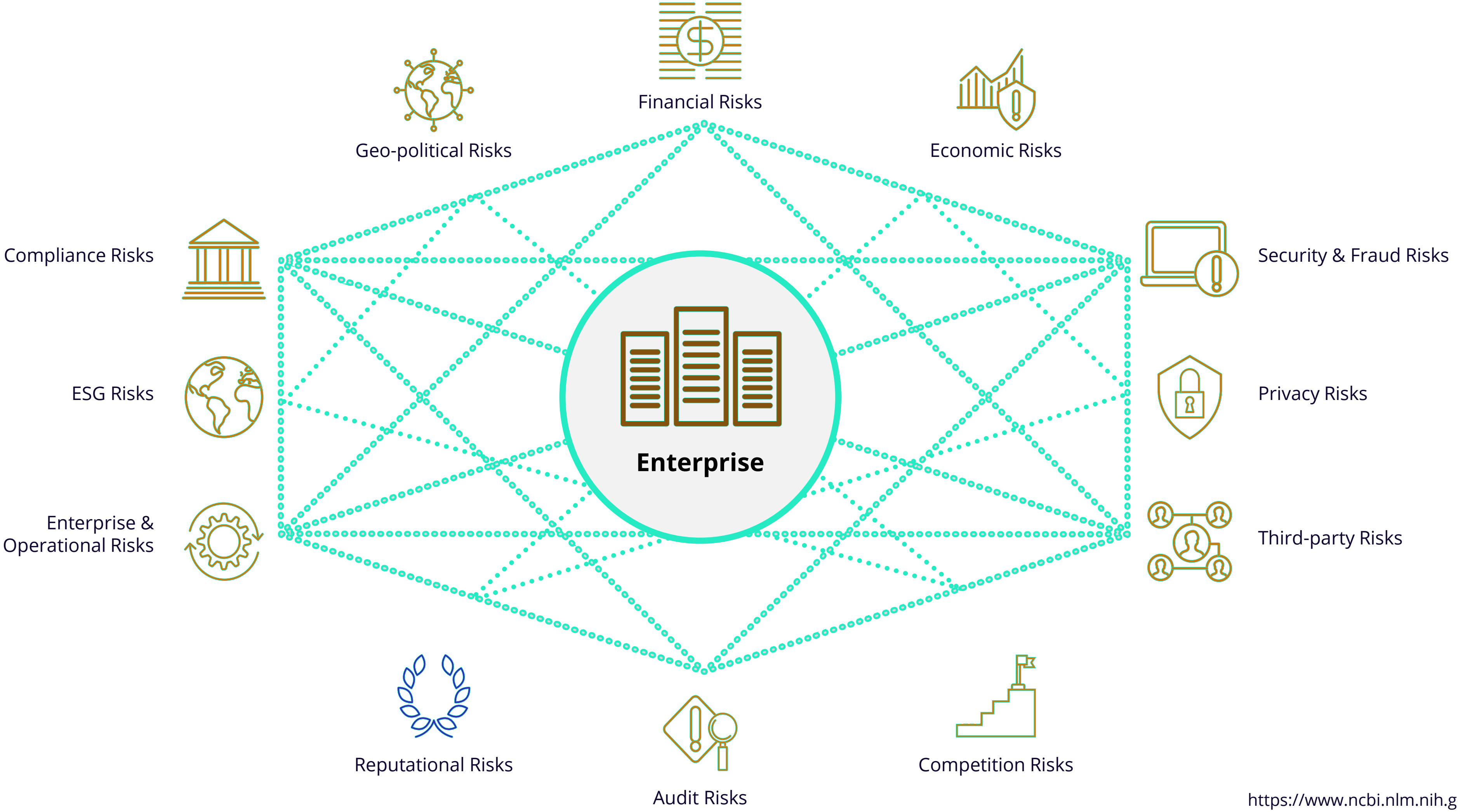
Current Market Situation

Shifts in GRC Challenges & Approaches

A new normal for turbulent times

- Connected risks
- Persistent challenges
- Coping strategies

Connected Risks



Financial Risks

Geo-political Risks

Economic Risks

Compliance Risks

Security & Fraud Risks

ESG Risks

Enterprise

Privacy Risks

Enterprise & Operational Risks

Third-party Risks

Reputational Risks

Competition Risks

Audit Risks

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/

https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/

Disruptions

It is an inevitable risk for firms to suffer disruptions to their operations as a result of natural or manmade disasters. Some of these could be, but not limited to

- Force Majeure
- Pandemic
- Cyber Attack
- Competition
- Litigations

Disruptions can be managed well if Enterprise can address its weakness around

- Processes
- People
- Systems
- External Events

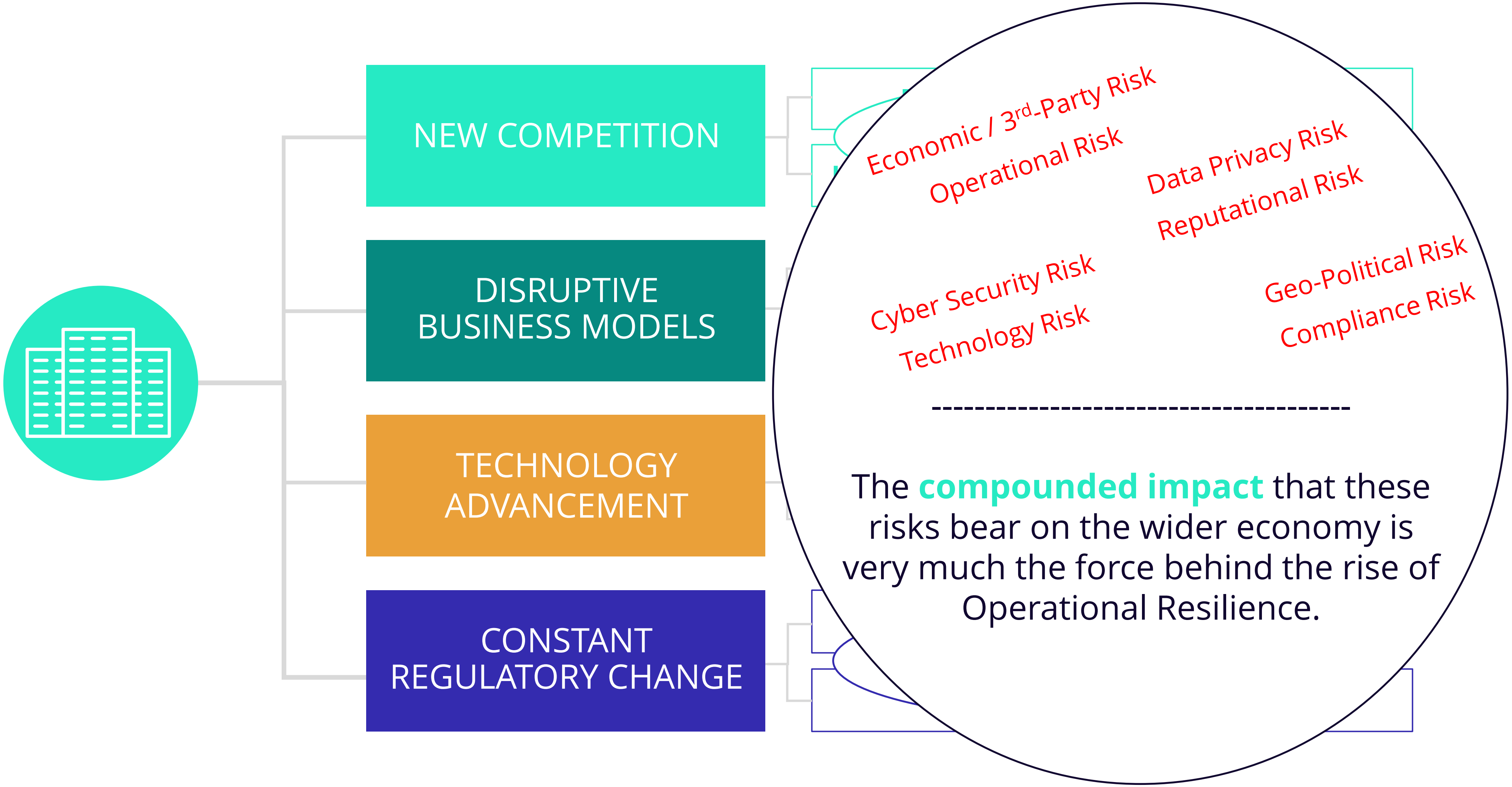
What is Operational Resilience

- Operational Resilience is the structured approach by which an Enterprise can Respond, Retrospect, Course correct and Move forward as an answer to disruptions.
- It is the principle that allows Organizations to Thrive on Risk.

Everyone deals with adversity; It's how you bounce back from it.

- Daniel Cormier

Operation Resilience – Key drivers



NEW COMPETITION

DISRUPTIVE BUSINESS MODELS

TECHNOLOGY ADVANCEMENT

CONSTANT REGULATORY CHANGE

Economic / 3rd-Party Risk

Operational Risk

Data Privacy Risk

Reputational Risk

Cyber Security Risk

Technology Risk

Geo-Political Risk

Compliance Risk

The **compounded impact** that these risks bear on the wider economy is very much the force behind the rise of Operational Resilience.

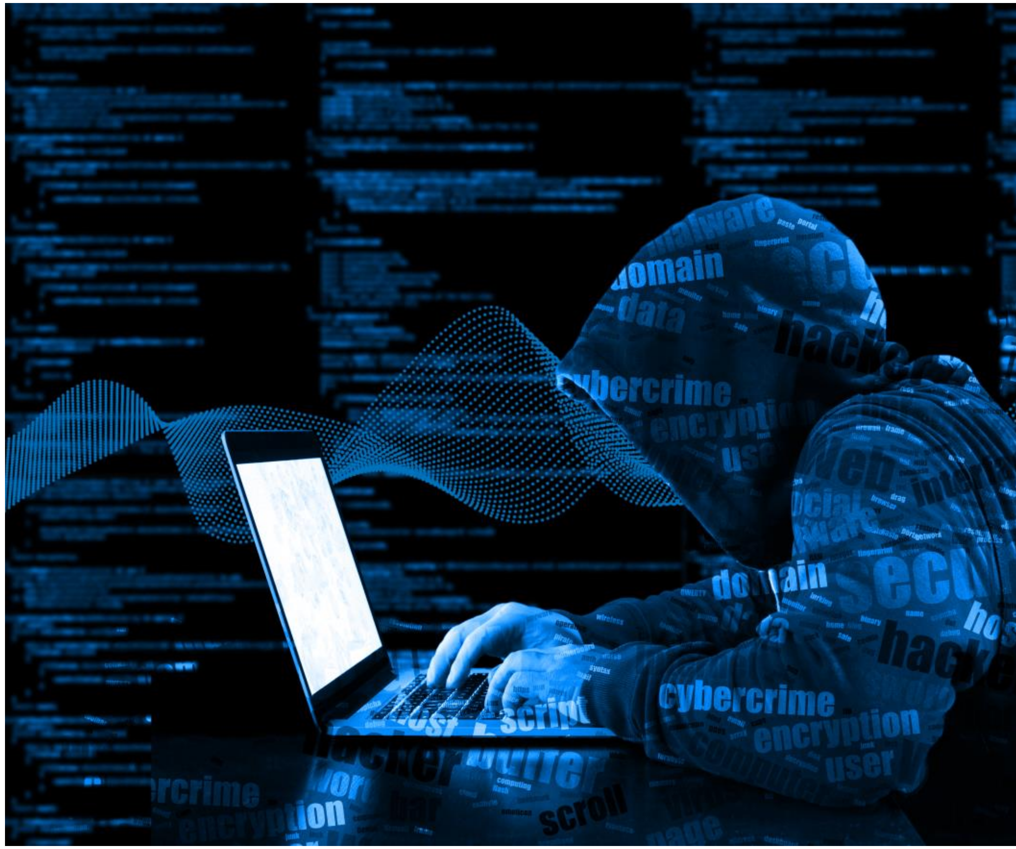
Regulatory Focus Around the World

Region	Regulatory Body	Details
Global	FSB FINANCIAL STABILITY BOARD	- The FSB's work program for 2023 includes Cyber and operational resilience
Americas	Office of the Comptroller of the Currency FEDERAL RESERVE SYSTEM UNITED STATES	- The OCC has issued guidelines on operational risk management, including resilience and business continuity. - The Fed has included operational resilience considerations in its supervisory expectations for banks and financial institutions.
UK & Europe	FCA FINANCIAL CONDUCT AUTHORITY European Commission BANK OF ENGLAND PRUDENTIAL REGULATION AUTHORITY EUROPEAN CENTRAL BANK	- European commission introduced Digital Operational Resilience Act (DORA) to improve the cybersecurity and operational resiliency of the financial services sector - The PRA and FCA have introduced operational resilience requirements for all financial institutions
Others	MAS Monetary Authority of Singapore APRA HONG KONG MONETARY AUTHORITY 香港金融管理局	- MAS has issued guidelines and regulations on operational risk management and business continuity for financial institutions - APRA regulates banks, insurers, and superannuation funds - HKMA has issued guidance on operational resilience for authorized institutions.

Colonial Pipeline Cyberattack

Operational Resilience: Lessons Learned

- The Colonial Pipeline was shut down for several days after a cyberattack by a ransomware group called DarkSide
- The shutdown caused widespread gasoline shortages and price increases in the affected areas
- Lessons Learned:
    - Critical infrastructure systems are vulnerable to cyberattacks.
    - Critical infrastructure systems need to have strong cybersecurity measures
    - The public and private sectors need to coordinate better in responding to cyberattacks.

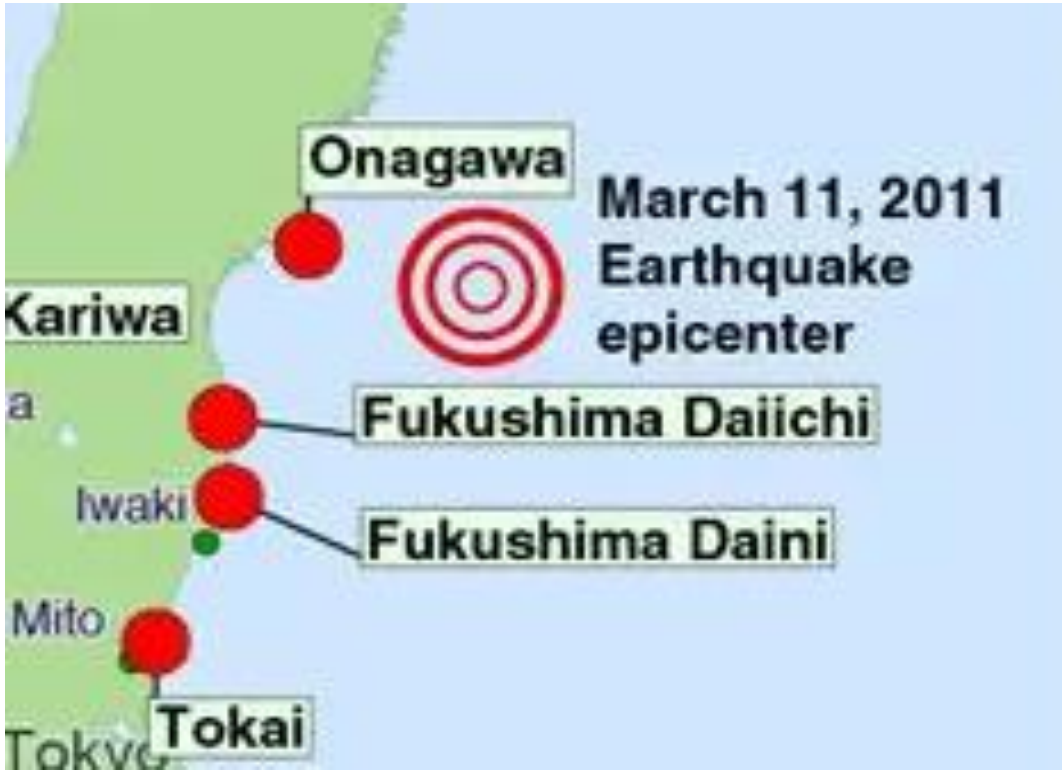


https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Japan Tsunami & Onagawa Nuclear Plant

Operational Resilience: In Action

- Fukushima and Onagawa are of the same approximate age and disaster conditions
- Fukushima Daiichi experienced **meltdowns** and **radiation** leakage
- Onagawa, being 40 miles closer to the epicenter was **undamaged** after experiencing higher ground motion, a larger wave. Why?
  - A proactive and collaborative culture of safety and risk awareness is a priority across the company
  - Strict protocols for disaster response, testing controls, and employee awareness on their roles and responsibilities



https://thebulletin.org/2014/03/onagawa-the-japanese-nuclear-power-plant-that-didnt-melt-down-on-3-11/
https://www.theatlantic.com/ideas/archive/2022/03/fukushima-nuclear-disaster-management-onagawa/627070/

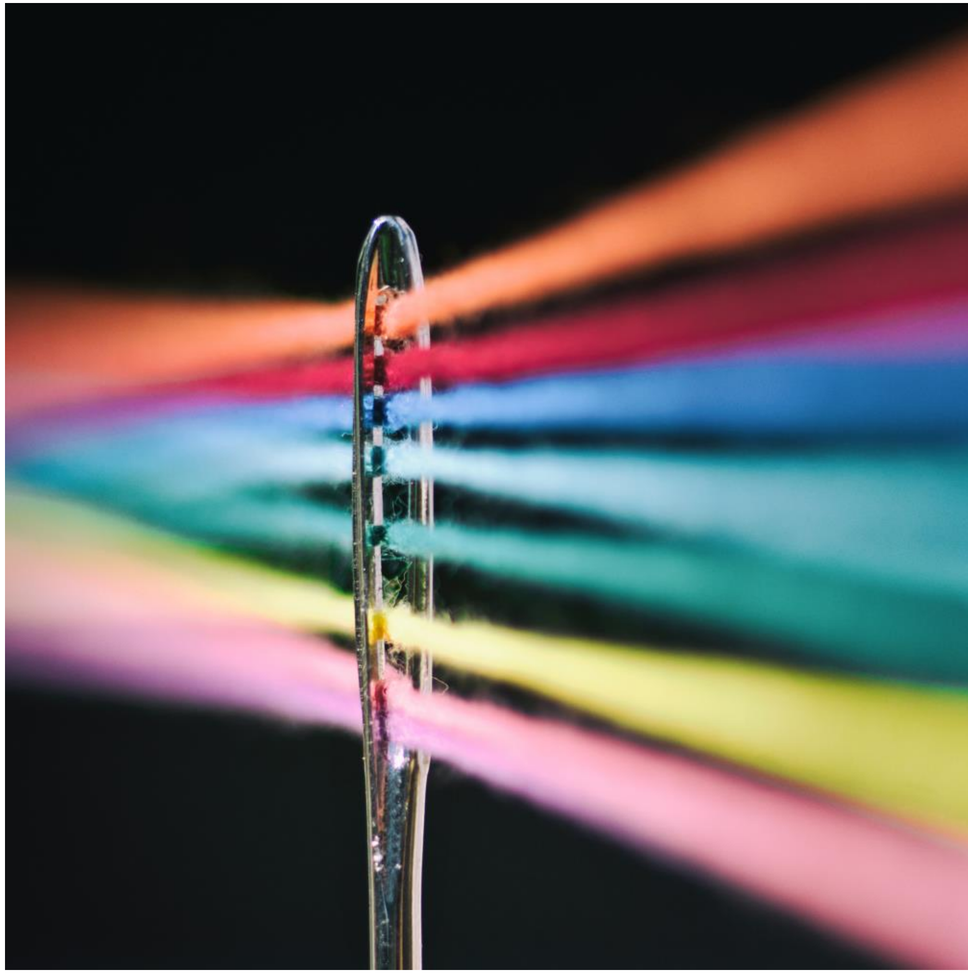
How to become Resilient?

1. **Disruption Absorption**

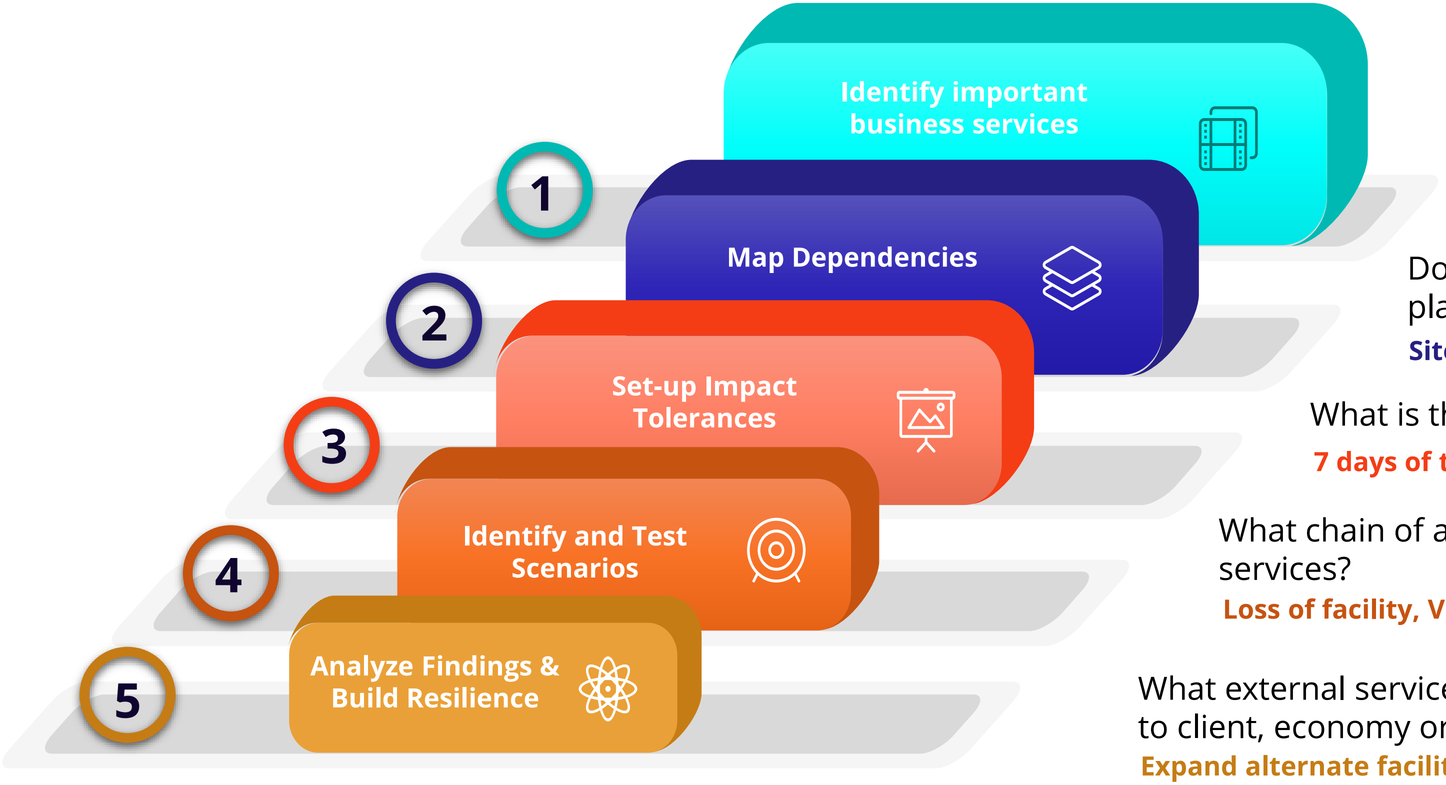
   Ability of a firm to maintain the structure and normal functioning of operations in the face of disruptions

2. **Recoverability**

   Ability of a firm to restore operations to a prior normal level of performance after being disrupted



Operational Resilience: Components


1
Identify important business services
2
Map Dependencies
3
Set-up Impact Tolerances
4
Identify and Test Scenarios
5
Analyze Findings & Build Resilience

Where are your gaps? What improvements should you make? How are you trending over time?

Settlement Transactions, Equities Trading, Credit Card Services

Do you remember within impact tolerance in the event of severe but plausible disruptions?

Site/location, Process & Business, Functions, IT Systems, Vendor Services

What is the maximum tolerable level of disruption?

7 days of total disruption, >$100M in direct financial impact

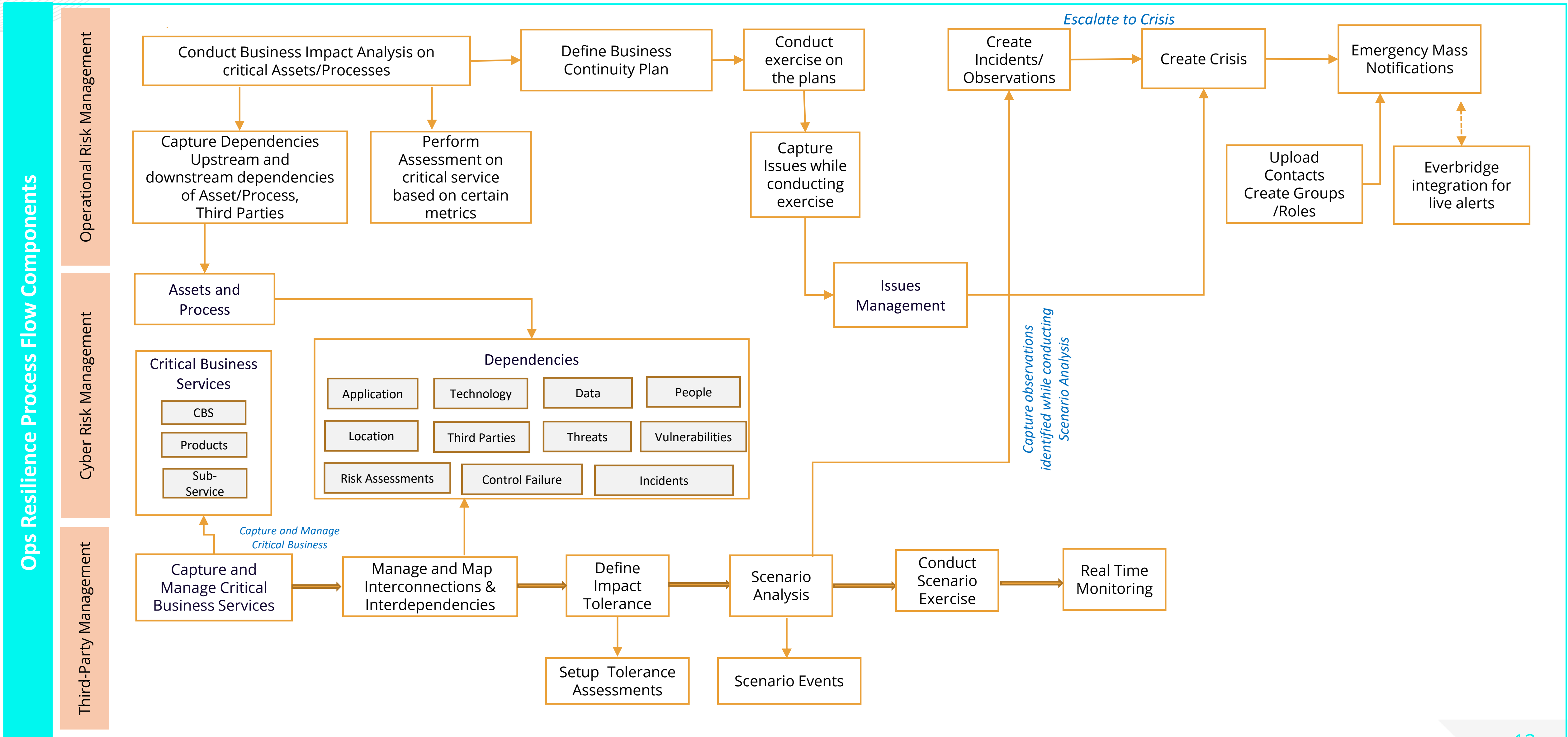
What chain of activities are involved in delivering those important critical services?

Loss of facility, Vendor, IT Systems, People due to extreme weather, Pandemic or Cyber attack

What external services do you provide customers where if disrupted could pose a risk to client, economy or firm?

Expand alternate facility or WFH establish alternate third-party

Operational Resilience



Ops Resilience Process Flow Components

Operational Risk Management

Cyber Risk Management

Third-Party Management

Conduct Business Impact Analysis on critical Assets/Processes

Define Business Continuity Plan

Conduct exercise on the plans

Capture Dependencies Upstream and downstream dependencies of Asset/Process, Third Parties

Perform Assessment on critical service based on certain metrics

Capture Issues while conducting exercise

Issues Management

Escalate to Crisis

Create Incidents/ Observations

Create Crisis

Emergency Mass Notifications

Upload Contacts Create Groups /Roles

Everbridge integration for live alerts

Capture observations identified while conducting Scenario Analysis

Assets and Process

Critical Business Services

- CBS
- Products
- Sub-Service

Dependencies

Application	Technology	Data	People
Location	Third Parties	Threats	Vulnerabilities
Risk Assessments	Control Failure	Incidents	

Capture and Manage Critical Business

Capture and Manage Critical Business Services

Manage and Map Interconnections & Interdependencies

Define Impact Tolerance

Setup Tolerance Assessments

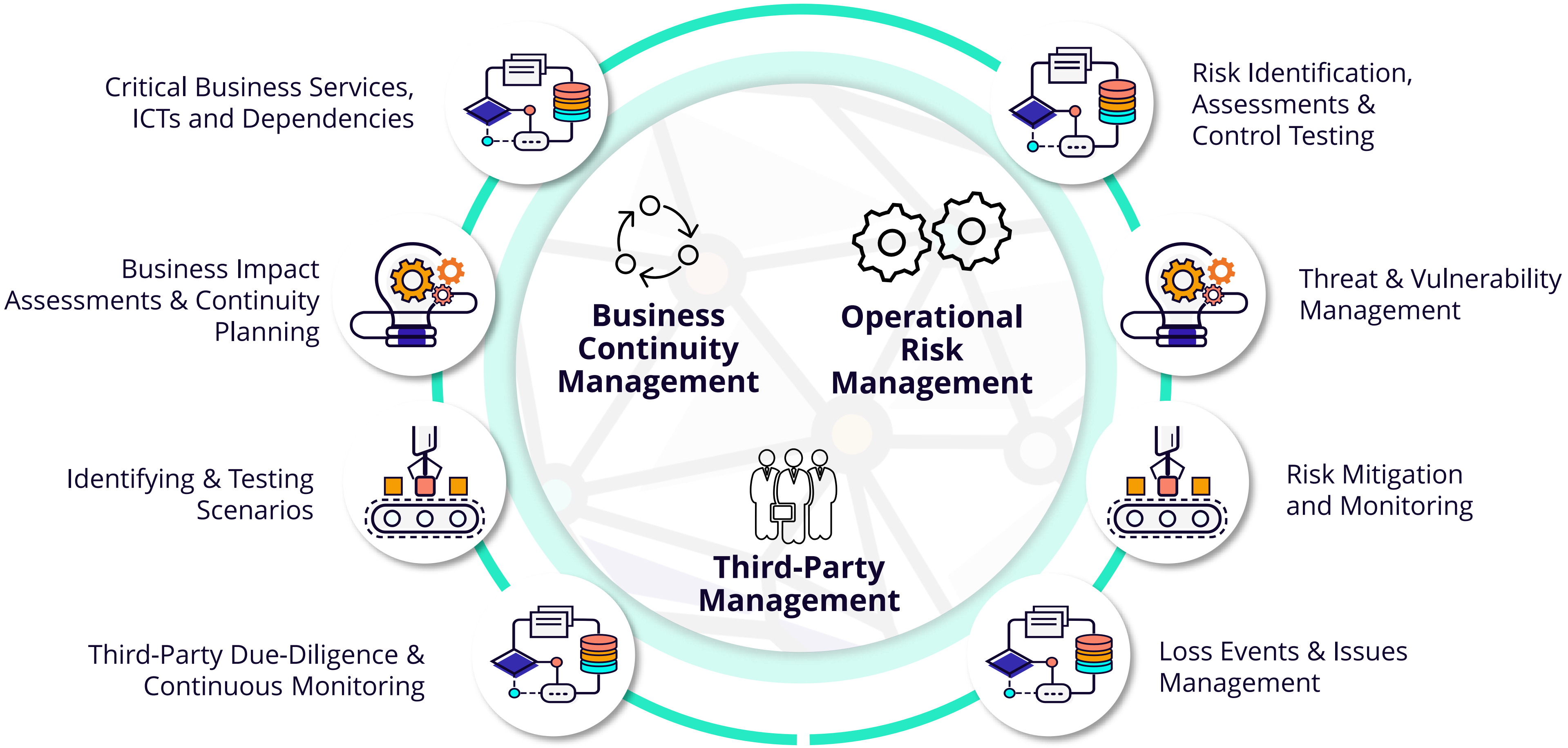
Scenario Analysis

Scenario Events

Conduct Scenario Exercise

Real Time Monitoring

MetricStream: Operational Resilience



Critical Business Services, ICTs and Dependencies
Business Impact Assessments & Continuity Planning
Identifying & Testing Scenarios
Third-Party Due-Diligence & Continuous Monitoring
Business Continuity Management
Operational Risk Management
Third-Party Management
Risk Identification, Assessments & Control Testing
Threat & Vulnerability Management
Risk Mitigation and Monitoring
Loss Events & Issues Management

GRC
SUMMIT 2023
MIAMI, JUNE 14 & 15
Hosted by MetricStream

Gratitude, Questions and Next Steps

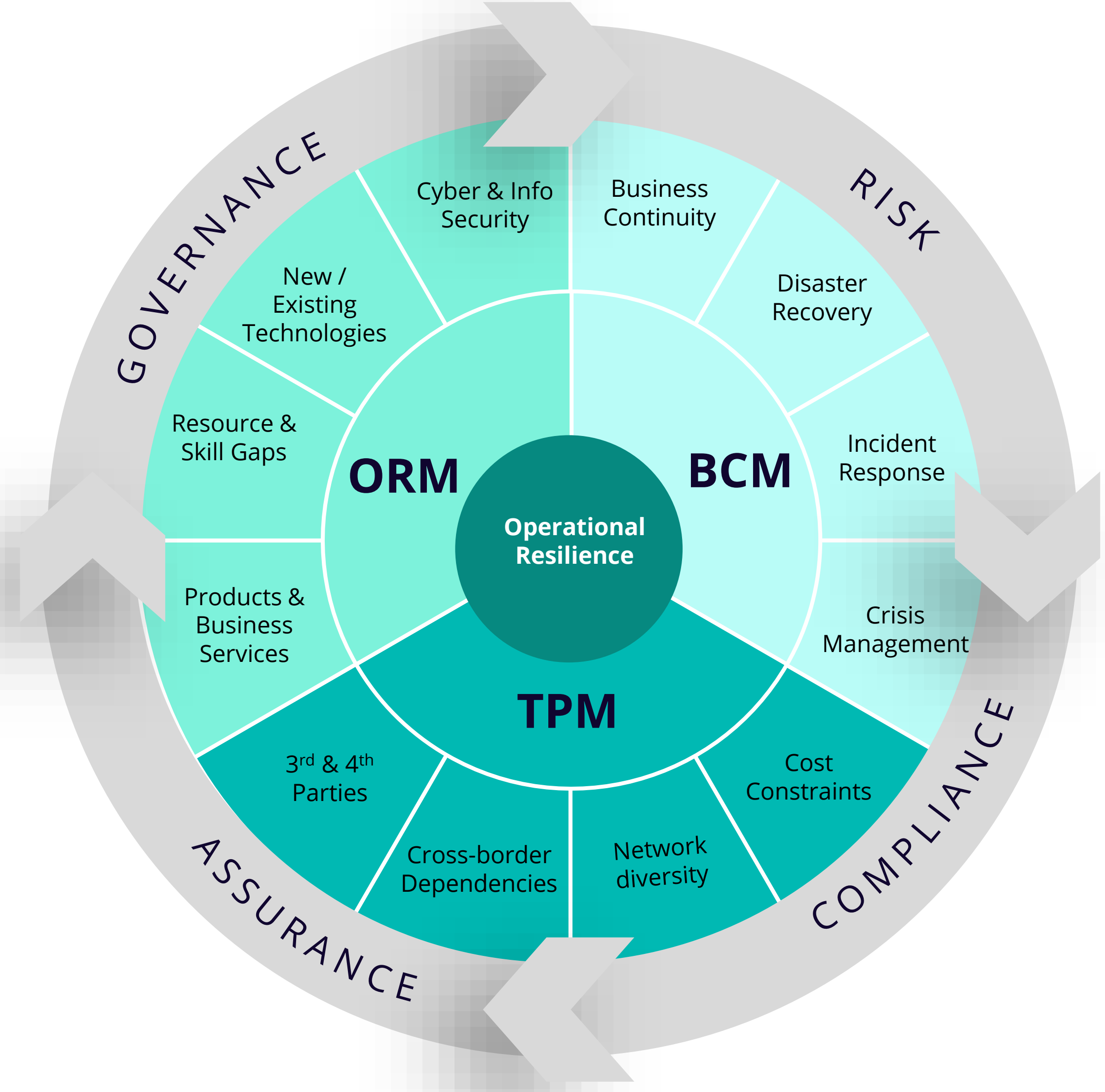
metricstream
thrive on risk™

GRC SUMMIT 2023
MIAMI, JUNE 14 & 15
Hosted by MetricStream

EXPERIENCE
the Power of Connection

Demonstration

Operational Resilience: <TITLE>

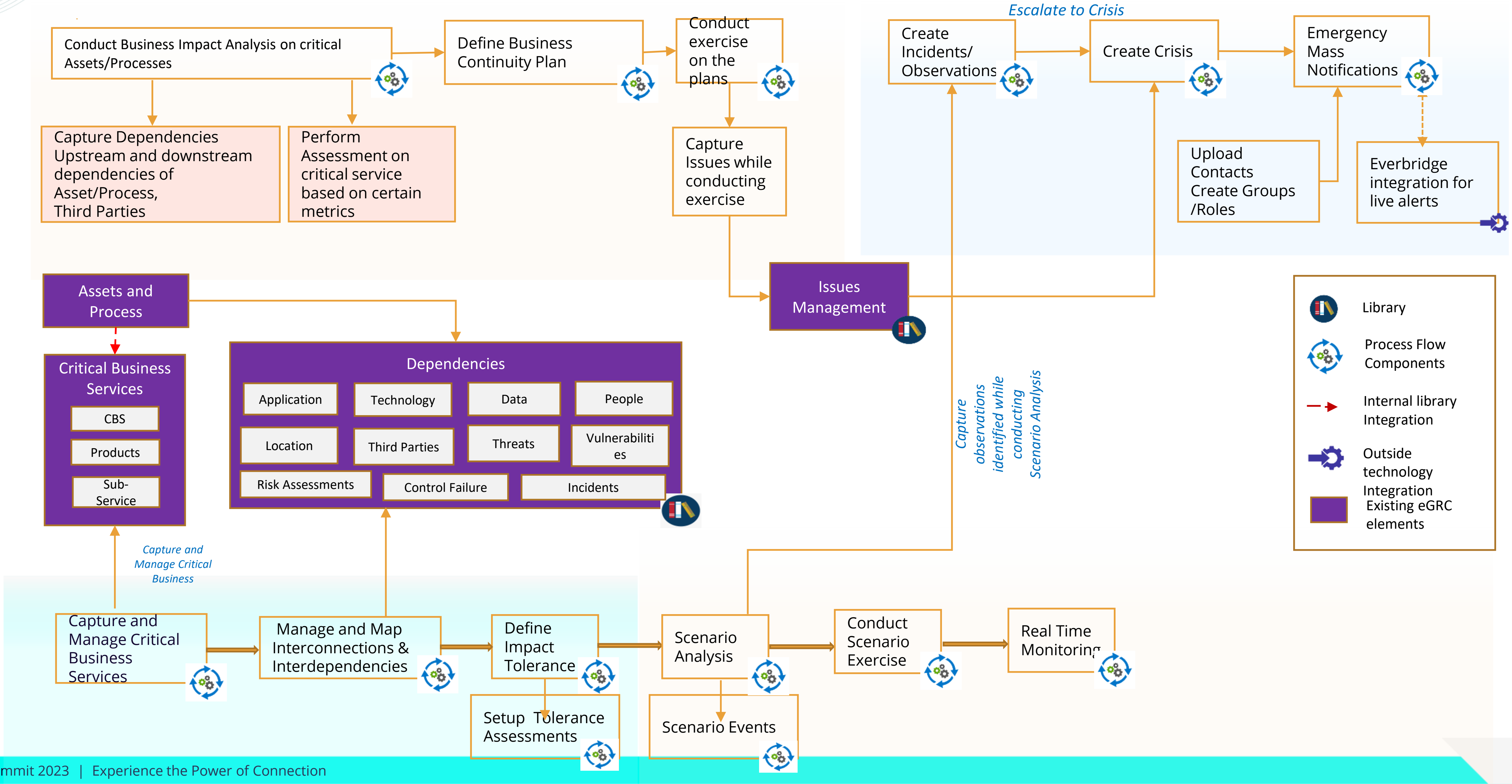


Organizations must succeed at:

- Managing the **interconnectedness** of all risk components
- Allowing **proactive management** of risks and associated mitigation activities
- Creating **organizational transparency** i.e. 'single version of the truth"
- Promoting increased **awareness/engagement** amongst organizational stakeholders
- Creating a pervasive **resilience culture**

MetricStream: Operational Resilience

Ops Resilience Process Flow Components



Conduct Business Impact Analysis on critical Assets/Processes

Define Business Continuity Plan

Conduct exercise on the plans

Capture Dependencies Upstream and downstream dependencies of Asset/Process, Third Parties

Perform Assessment on critical service based on certain metrics

Capture Issues while conducting exercise

Escalate to Crisis

Create Incidents/ Observations

Create Crisis

Emergency Mass Notifications

Upload Contacts Create Groups /Roles

Everbridge integration for live alerts

Issues Management

Assets and Process

Critical Business Services

CBS

Products

Sub-Service

Dependencies

Application	Technology	Data	People
Location	Third Parties	Threats	Vulnerabilities
Risk Assessments	Control Failure	Incidents	

Capture observations identified while conducting Scenario Analysis

Capture and Manage Critical Business

Capture and Manage Critical Business Services

Manage and Map Interconnections & Interdependencies

Define Impact Tolerance

Setup Tolerance Assessments

Scenario Analysis

Scenario Events

Conduct Scenario Exercise

Real Time Monitoring

Library

Process Flow Components

Internal library Integration

Outside technology Integration

Existing eGRC elements

Tips for improving operational resilience:

1. Risk Assessment and Management:

- Conduct thorough risk assessments to identify potential vulnerabilities and risks across all aspects of operations.
- Regularly update and refine risk management strategies and processes based on changing business environments and emerging threats.
- Implement risk mitigation measures, such as redundancies, diversification of suppliers, and comprehensive business continuity plans.

2. Robust Governance and Compliance:

- Establish strong governance frameworks to ensure clear accountability, decision-making processes, and oversight of operational resilience efforts.
- Stay informed about regulatory requirements and industry best practices to maintain compliance and address emerging challenges.
- Regularly assess and audit operational resilience practices to ensure adherence to standards and identify areas for improvement.

3. Technology and Infrastructure:

- Implement robust and secure technology solutions to protect critical systems, data, and infrastructure from cyber threats and physical disruptions.
- Regularly update and patch software systems to address known vulnerabilities and stay up to date with the latest security measures.
- Utilize automated monitoring and alerting tools to promptly detect and respond to potential disruptions.

Tips for improving operational resilience Contd..

5. Collaboration and Partnerships:

- Establish partnerships and collaborations with external stakeholders, such as industry peers, regulators, and cybersecurity experts, to share best practices and insights.
- Engage in information sharing initiatives to stay informed about emerging threats, vulnerabilities, and effective resilience strategies.
- Participate in industry forums and working groups to contribute to the development of resilience standards and guidelines.

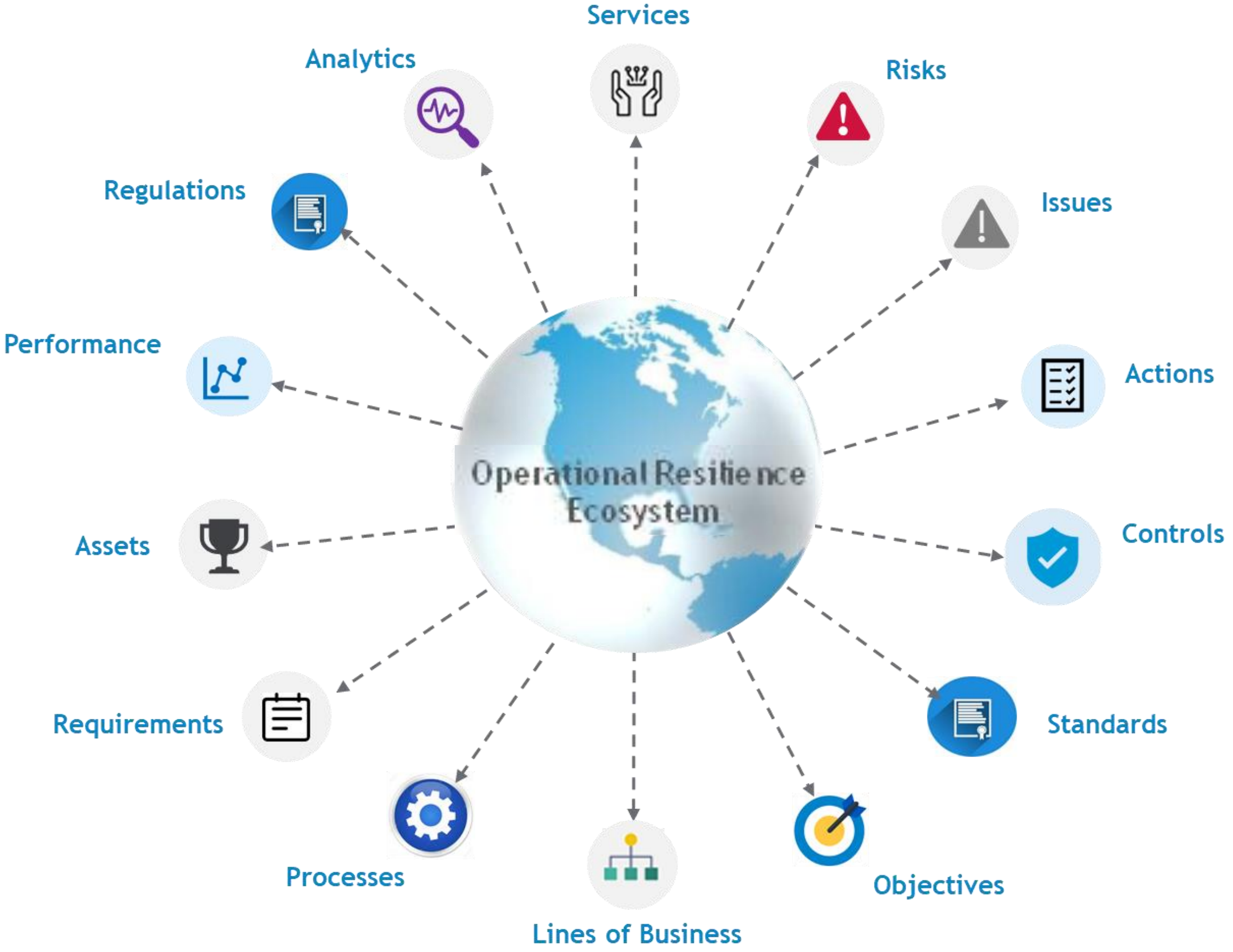
6. Continuous Improvement and Testing:

- Regularly review and update operational resilience plans, procedures, and processes based on lessons learned from incidents, near-misses, and changing business conditions.
- Conduct periodic testing and simulations of various disruption scenarios to assess the effectiveness of operational resilience measures.
- Continuously monitor and analyze operational resilience performance metrics to identify areas for improvement and take proactive measures to address them.

Operational Resilience Practices

- Consistency and standardization
- Interconnectedness and Interdependencies
- Regulatory Compliance
- Efficiency and Effectiveness
- Strengthening the Ecosystem

The Power of Integrated Governance & Risk Programs



Integration provides a powerful platform that:

- ❑ Brings together all the many **interconnected components**
- ❑ Allows **impact evaluation** on evolving business eco-systems
- ❑ Allows **target recalibration** to adapt to business demand changes
- ❑ Promotes **organizational learning** where root causes and mitigation activities can be better managed