Operational Resilience in Real Time: The New Imperative for Financial Services

Resilience is the ability of an organization to continue to serve its customers, deliver products and services, and protect its workforce in the face of adverse events. Operational resilience gives banks the ability to simplify and streamline technologies supporting important business services, leading to better customer outcomes, even during unexpected service outages. Despite understanding this need, resilience in the financial services industry is harder than ever. Disconnected operational processes, fragmented capabilities, rising cyberthreats, and ever faster regulatory change all contribute to greater challenges in maintaining resiliency. Understanding and mitigating the potential operational impact of each risk event and their cumulative or synergistic nature is key. This illustration offers a process that can be applied in any organization.

WHAT DOES RESILIENCE LOOK LIKE?

- Establish indicators, controls, communication & response plans, and monitoring systems
- Evaluate communication and training effectiveness and test event scenarios
- Monitor risk indicators and events, both internal and external
- Update controls and plans as often as needed to support changing priorities and conditions

The organization has confidence to manage through automation-enhanced processes. Disruption in business continuity planning give way to enterprise-wide, siloed and manual crisis communications and customer facing interactions.

Digital transformation addresses back end systems and reliance on a common data model and workflows. Business processes and capabilities are mapped to operational resilience depends on four key pillars of the business. The support processes for the reliable delivery of services and products. The business technology must always be available and secure. The workforce must be kept safe and in compliance with all requirements. Third party risks must be known and controlled while ensuring performance.

PILLARS OF OPERATIONAL RESILIENCE

1. ANTICIPATE
- Inventory customers, critical products & services, assets, personnel, facilities, vendors
- Identify risk dependencies & potential related impacts
- Prioritize risks based on likelihood, business impact & established tolerances
- Establish thresholds and tolerances for each risk to be addressed

2. PREVENT
- Establish indicators, controls, communication & response plans, and monitoring systems
- Evaluate communication and training effectiveness and test event scenarios
- Monitor risk indicators and events, both internal and external
- Update controls and plans as often as needed to support changing priorities and conditions

3. RESPOND / RECOVER
- Respond to adverse events
- Communicate accurately to stakeholders and participants
- Restore operations, services, systems & processes

Our comms plan says the next thing to do is set up a crisis bridge and notify our C Suite and Board

4. ADAPT
- Identify root causes
- Implement new or updated controls & metrics

New controls for each pillar in isolation with siloed data or controls...set and forget assessments, plans, or controls...wait to make needed adjustments until annual review

How can we best control the risk of our critical vendors?

DO

- ...treat operational resilience as a shared mission across stakeholders
- ...use business impact and risk to prioritize and direct resources throughout the cycle
- ...replace manual, paper, repeated processes with digitized workflows and continuous monitoring

DON'T

- ...treat each pillar in isolation with siloed data or controls
- ...set and forget assessments, plans, or controls
- ...wait to make needed adjustments until annual review