Resiliency and Risk Management

December 2021

This publication is sponsored by the members of the North American CRO Council. Council members represent Chief Risk Officers of leading insurers based in North America, who as a group, aim to provide thought leadership and direction on the advancement of risk management, and risk-based solvency and liquidity assessments. The content of this publication reflects the views of the majority of the Council, and not necessarily the opinion of every member.

Introduction

Resiliency is a proactive, strategic approach for day-to-day practices, positioning an organization to manage operational risks in a way that enables continuous delivery of services with minimal to no disruption. Resilient organizations proactively prepare to minimize the impact of potential risks to business objectives and react and adapt quickly to events. Operational resiliency has moved beyond traditional Business Continuity planning by integrating the various recovery and resiliency efforts within an organization (i.e., Business Continuity / Disaster Recovery, Crisis Management, Incident Response, Information / Cyber Security, Third Party Management, IT Automation, etc.). This paper identifies three pillars for a resilient organization; Resilient Business Operations, a Culture of Preparedness, and Third-Party Resiliency.

Although Business Continuity programs are a component of a resilient organization, business continuity focuses on recoverability of siloed business processes and systems, rather than sustainability and adaptability of end-to-end business services, which may ignore critical components within the value chain. The standard set of business disruption scenarios may give a false sense of comfort that the company is prepared for all scenarios.

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 (FFIEC Sound Practices to Strengthen Operational Resilience). There is a growing interest in the concept of resiliency due to the heightened risk associated with large scale natural disasters, pandemics, increasing digitalization of products and services, supplier dependency, and advancements in the cyber threat landscape. Benefits of a robust operational resilience program include improved customer confidence, lower impact and costs from adverse events, and the ability to meet current and future regulatory requirements.

Resilient Business Operations

An organization should have a formal methodology to identify and document critical business processes and process flows, third-party dependencies, and IT asset relationships. This information can be used to prioritize business resiliency activities, identify critical steps and solutions, and help guide the selection and management activities of third-parties. A resiliency program should provide a set schedule to review the design, relevance, and criticality of the business processes.

Business Architecture

Resilience work should be prioritized based on what is most critical to the success of the business, which requires thoughtful business architecture defining the primary objectives of the business, and the business processes executed to achieve them. Each business process should be clearly identified and documented, consistently scoped, and prioritized by criticality, aligning to the criticality of the related business objectives.

To understand the criticality, resiliency professionals must understand the intended audience of each business service, the ways they will be accessed, and the stakeholders providing the service and benefitting from the service. All of these are needed to understand

service dependencies, requirements of upstream and downstream processes, and potential risks associated with the objectives.

Business Process Design

Once the high level business architecture is determined, the organization will define the business processes related to each business service. Business processes are enabled by people, infrastructure, and technology, and all of these should be accounted for when planning for and designing process operational resilience. The architecture of each business process should be documented end-to-end, including all process activities, the people who perform them, and the technology that enables them, including both customer-facing systems and internal organizational infrastructure (network, servers, storage, etc.)

To understand the criticality of a business process, resiliency should be considered for the entire business process, from start to finish, and for all the pieces that enable the process, including (but not limited to):

- Manual workarounds that can be used if the normal technology is impacted by an event
- Identification of all the technology required for the business process to operate, including third parties
- Training, hiring, retention, and management of the people who provide, support, and govern the business process
- Service Level Agreements and Operational Level Agreements, including support objectives
- Resiliency expectations to be included in contract terms with third party providers as appropriate
- Process to Process relationships documented and the integration understood by the process owners and parties involved in providing the process

Business Impact Assessment (BIA)

Many companies use a BIA as part of their Business Continuity and Disaster Recovery planning. A well designed BIA can remove much of the subjectivity of determining process criticality. Once the company has determined what the most critical business processes are, based on responses in the BIA, then the lower level resilience and recovery requirements become clearer.

Business Process Inventory

Once the BIA has been completed, the results can be applied to the design and architecture of the solutions that enable the business process, such as the people, infrastructure, and technology. All of this information should be documented in a business process inventory.

Having a well-defined business process inventory allows leaders to overcome departmental boundaries to obtain a holistic view of business processes (end-to-end) to create efficiency, improve customer experience, and facilitate effective risk management. A business process inventory provides stakeholders the ability to take a risk-based approach to:

- Identify interdependencies of internal business processes, business applications and IT infrastructure, third parties, facilities (including remote workers).
- Define recovery priorities and resource dependencies for critical processes
- Promote operational resiliency by mitigating vulnerabilities associated with critical processes
- Understand where the most sensitive data is being used to comply with industry regulations and standards
- Understand key contractual obligations

for your Clients that could be impacted by a disruption
- Measure customer related activities and outline customer experience
- Improve efficiency through process standardization to perform processes that add business value
- Streamline communication and collaboration between people / functions / departments / third parties
- Establish accountability and optimum use of resources for relevant processes

Culture of Preparedness

Once the needs of the business are thoroughly understood, the company can identify threats, risks, and risk mitigants for business process and associated dependencies. Business continuity management, disaster recovery planning, cyber risk management, and scenario exercises can help promote an organizational culture focused on resiliency.

Business Continuity Management

Business Continuity Plans (BCPs) should include strategies that enable response to a variety of relevant scenarios, either enterprise-wide (e.g., pandemics, technology) or specific to individual operations. BCPs should include remote work strategies as well as considerations for returning to normal operations after a disruption. BCPs should document essential personnel to include both company and third-party personnel that are critical for delivery of critical business services.

The BIA can be used to gather information about the resiliency needs of a business process in addition to identifying recovery and continuity strategies. Any manual workarounds that can be used to continue to provide business services during a significant outage should be documented in detail.

BCPs should be aligned to the guidance provided by a Business Continuity Policy and be regularly reviewed and updated, in addition to being regularly exercised (including tests of workarounds, recovery, and processing). BCPs should be updated after each exercise based on lessons learned. Exercises may also provide lessons learned for improving the resiliency or recovery of a business process. Plan exercises should demonstrate whether resiliency objectives are being met. Exercises should increase in scope and complexity over time to continually provide assurance for the continuity and resilience of critical business processes. Any significant gaps identified as part of the exercise should be logged and management action plans tracked for resolution prior to the next exercise.

BCPs should be documented at a level of detail that would enable someone unfamiliar with the process to perform the activities documented, and integrated effectively with Disaster Recovery, Crisis Management, and other resiliency-related programs. The plans should define continuity, recovery, and restoration objectives based on the risks identified in the BIA, as well as aligning with the criticality and priority of the service being provided.

Disaster Recovery Program

Resiliency revolves around creating technical solutions, from infrastructure to applications, that can withstand or prevent loss of services due to an unplanned event. Disaster recovery concerns the restoration of normal operations after an unplanned event. Disaster Recovery program, strategy, and technical recovery plans should align to the Business Continuity strategy and plans. Disaster Recovery plans should align to program policies and standards and should be based on

business driven prioritization. Disaster Recovery plans also need to be well documented, with clear roles and responsibilities, and tested on a regular basis.

Cyber Resiliency

The number of cyber events continues to increase sharply, leading to a widespread recognition that some cyber events cannot be stopped. As a result, organizations have started to improve their prevention capabilities while augmenting their cyber event detection and response capabilities. It is imperative that companies review current measures for greater awareness and understanding of how technology, facilities, people, and processes are leveraged to achieve resiliency. Disciplines of prevention, detections, and response that have long been included in cyber, can be applied more broadly.

The Cyber Risk Management program should include elements for resiliency, including proactive and reactive resiliency processes—identifying and assessing both internal and external threats, and developing plans to either avoid the threat or minimize the impacts. Controls should be established to maintain the integrity and availability of data against the impact of cyber threats, such as ransom ware. The cyber risk landscape changes frequently, and cyber-resiliency plans should be updated regularly, exercised often, and continuously improved based on lessons learned during exercises.

Cyber risks should be identified and assessed with considerations for people, facilities, technology, and third parties. This includes robust training for employees to understand phishing or pretext calling as well as technical protections like firewalls, patches, and ongoing monitoring.

Two specific, increasingly common cyber threats that may impact operations are ransomware and denial of service attacks. Companies should ensure that risk controls are in place to prevent, detect, respond, and recover from these threats. Potential impacts include voice-over-IP (VoIP), email, internet, remote access / virtual private network (VPN), file transfers, and integration with third parties. Companies should consider scenarios that explore alternatives for regional service providers, such as dedicated lines for critical third party services.

Well planned and architected data protection and recovery are crucial when it comes to withstanding a cyber attack. While DDoS and Ransomware attacks are generally easy and quick to detect, other types of cyber attacks like data theft or changes may not be detected for months, requiring alternate risk mitigation.

Scenario Planning Exercises

A resiliency program is a specialized risk management practice focused on avoiding outages and recovering quickly from outages. This can include (but isn't limited to):

- Aligning risk assessments to business processes to enable an aggregate view of operational risks impacting business operations.
- Executing risk management activities at all levels of the organization and in all applicable activities and programs.
- Clearly defining roles and responsibilities for identification and management of operational risks.
- Providing oversight to help ensure consistent and reliable resiliency validation activities across business areas, business continuity management, cyber and IT recovery.
- Use Business Impact Analysis (BIA) output, risk assessments, and lessons learned from actual events to develop

realistic scenarios to effectively test recovery and resiliency capabilities.
- Coordinate scenario planning and testing activities across business areas, business continuity management, cyber and IT recovery to consistently assess risks.

Third-Party Resiliency

Understanding and managing the dependency on third-parties, especially in the risk of critical dependency on a single third party / vendor, is an important piece of overall resiliency. A third party poses greater risk if the third-party is unable to provide the service in a resilient enough way to meet organizational resiliency objectives, and / or there are no other third-parties to fall back on for the service being provided, creating a single point of failure.

Third party risk can be mitigated in different ways depending on the nature and criticality of the service provided:
- Understand the business continuity approach of the third party, including how they design for resiliency and how they exercise their business continuity and disaster recovery plans
- Consider whether the provider's continuity and recovery objectives are in line with the requirements of the business, and whether this poses a risk that must be addressed
- Work with the third parties to design geographic redundancy to avoid location-specific issues
- Identify alternate third parties that could provide the service if the main provider becomes unavailable
- Temporarily bringing a service back in-house when a third party provider is unavailable

Conclusion

Resiliency encompasses a holistic and strategic risk management framework which requires ongoing diligence as business operations and technology continue to evolve. Being weaved within the organization's culture, resiliency requires an integrated approach across the company including business areas, information technology, information security, third party management, facilities administration, and risk management practitioners to be successful. An organization should have a formal methodology to identify and document critical business processes and process flows, third-party dependencies, and IT asset relationships.

Although some business disruptions may be unavoidable, steps can be taken to reduce the risk of prolonged impact through Crisis Management, Business Continuity planning, proactive IT development, and scenario exercises considering cyber and third party risks. Based on the size and complexity of an organization, a Resiliency Program should be considered to provide holistic governance, monitoring and reporting of the various aspects of resiliency risks.