RSA

WHITE PAPER

Key Principles In Building Operational Resiliency

It is hard to find an organization not impacted by the pandemic or other recent disruptions—whether natural, man-made or cyber disruptions, or a combination of several. Impacts from these events have resulted in employee health and safety issues, supply chain disruption, physical damage, loss of customers, reputational damage and increases in the cost of doing business—and the financial impacts have been astronomical.

Of all the disruptions in 2020 so far, the pandemic has impacted the most people, geographies and industries, including hospitality, travel, transportation, healthcare and retail. Opportunistic cyber breaches have also increased in 2020, impacting the safety, security and business value of organizations of all sizes, in all industries and locations.

Operational resiliency has become a regulatory, corporate and board-level topic within many organizations due to the liability and loss they have experienced and that has been inflicted on economies worldwide. The nature, frequency and magnitude of disruptions have caused organizations to evaluate their abilities to properly identify threats, analyze the risk and implement plans to avoid or recover from them. With the increasing frequency of disruptive events, it is impractical to rely on recovery alone.

Resources are spread thin even with one disruption, let alone concurrent events that tax not only the resiliency team but also the rest of the organization. To shift from a reactive to a proactive posture, resiliency must be built into the very fabric of the organization—from its culture to how the company operates both internally and across the extended third-party ecosystem.

> Resiliency cannot be the responsibility of a small group of people—everyone must have a role in building and practicing resiliency.

Operational resiliency

Operational resiliency is the ability of an organization to absorb changes and adapt in an evolving environment, so it can deliver its objectives, and survive and prosper. Operational resiliency includes, but is more than, business recovery; it is a change in mindset, culture and approach that drives the implementation of resilient measures and practices throughout and by the business.

Five key principles for building operational resiliency include:

- Prioritize important business services
- Implement an effective business continuity management system
- Build ownership across the organization
- Integrate resiliency and risk management
- Drive resiliency across third parties

Prioritize important business services

Every organization has a core mission and strategic objectives, and the products and services it provides—whether online banking, emergency surgery or on-time flights—constitute an important part of this. The organization has to assume that at some point the ability to provide these products or services will be interrupted.

A key question is how long the organization can tolerate a disruption before intolerable impacts occur. Intolerable impacts could include loss of a certain number of customers or missed transactions, or a day's worth of late flights. It's up to each organization to determine their impact tolerance.

To reduce intolerable impacts, the products and services most critical to the ongoing viability of the organization must be made resilient. Not everything can be made resilient at once; therefore, it is critical not only to prioritize but also to focus on the products and services the organization provides to customers, as well as what makes up these products and services—the supporting business processes, systems, people, assets, data and locations.

Implement an effective business continuity management system

An effective business continuity management system (BCMS) is a vital part of the strategy to build operational resiliency. A BCMS consists of a business continuity management (BCM) program, automated tools, human resources and reporting structure. A BCM program includes business continuity planning (BCP) and IT disaster recovery (ITDR); incident management, which is the routine handling of small, business-as-usual events before they become a crisis; and crisis management, which is the art and science of dealing with actual crisis events.

Even though BCP, ITDR, incident management and crisis management are the most common components of an organization's BCM program, they are often disconnected and performed by separate teams with different tools, objectives and approaches. Disruptions and crises result in enough damage by themselves, but the disconnected state of these teams can add to the risk, reduce speed to respond and result in more negative impacts.

Integrating BCM functions builds operational resiliency by better aligning the organizations that deal with disruptions, using approaches that are more fluid, practical, actionable and tested—and reduce intolerable impact to the organization.

Build ownership across the organization

Building operational resiliency must no longer only be the responsibility of the BCM program, but instead must be owned across the business—by each business unit and department, including IT, sales, public relations and more. Building operational resiliency may start with the BCM program but it will not thrive without proactive participation across the business in building operational resiliency into the organization's culture, processes, systems and practices.

A critical component is ownership of operational resiliency at the executive level. Executive ownership, such as by the chief operating officer (COO) or chief information officer (CIO), provides the importance, sponsorship and visibility to make and sustain progress against other business priorities.

Ownership by the COO shows that operational resiliency is owned by the business units, and it becomes a strategic objective directly tied to the organization's operating results. Ownership by the CIO is effective in an IT-driven business, as this reporting relationship can foster better innovation and integration across areas such as cloud, application development, IT support and ITDR.

Integrate resiliency and risk management

Risks that threaten the operational resiliency of an organization come in many forms—health crises, cyber threats, operational events and supply chain disruptions. In fact, risks impacting an organization can often cause a domino effect. For example, weak security controls in a third party may result in a cyber breach to the engaging organization. The breach may result in an exposure of customer data (a compliance violation) and result in a disruption of systems that requires IT disaster recovery. The interconnected nature of risks illustrated in this example demonstrates that risk management must be integrated across the organization and operational resiliency must be closely tied in—especially aligning on risk appetite, risk tolerance and a risk profile.

A challenge to this premise is that risk management is typically performed by separate functions across the organization, including third-party governance, IT, internal audit, operational risk and business resiliency functions. This approach, which has likely grown up over time, may put the spotlight on individual risks, but where C-suite executives and boards are asking frequently about the status of strategic risks, it makes rolling up those risks and reporting them at high levels very difficult.

All the functions performing separate risk management activities should align, if not organizationally, then at least using the same methodologies, risk tolerances and automated toolsets, so the results, reporting, dashboarding and monitoring of key risk indicators are more instantaneous and accurate when rolled up as strategic risks for executives. This type of risk management discipline will only strengthen the ability to build operational resiliency.

Drive resiliency across third parties

Third parties are an extension of the engaging organization and in some cases perform very critical functions for them. Internal and third-party organizations are often very closely intertwined in the delivery of products and services, and if one is disrupted, the other may be impacted too. Therefore, it is vital to ensure that third-party ecosystems, supply chains and other external partnerships are as resilient as the engaging organization. Myriad issues must be considered as organizations strive to build operational resiliency with individual third parties and across their unique third-party ecosystems.

Third-party ecosystems are becoming more complex and specialized. For example, organizations may become dependent on a small number of outsourced or third-party service providers who are very difficult or impossible to substitute, which could, over time, give rise to systemic concentration risks. A major disruption, outage or failure at one of these service providers could create a single point of failure with potential adverse consequences for financial stability. This can be especially true of cloud providers. In addition, sub-outsourcing to a third party's third parties (nth parties) can amplify certain risks in outsourcing arrangements, such as data security, and limit an organization's ability to manage them—particularly where large, complex chains of service providers are involved.

Third-party resiliency is complicated to achieve because the control and responsibility lie with the third party. However, there are ways to build toward operational resiliency of third parties. For example, during onboarding of a third party, service-level agreements and clauses can be included in contracts that stipulate the third party will take steps such as maintaining and testing their recovery plans. These agreements should cover how the third party will maintain operational resiliency under normal conditions and in the event of a disruption. Engaging organizations can also monitor the third party on an ongoing basis through performance and resiliency metrics, perform joint tests of resiliency measures and normalize procedures to align the resiliency of the third party with their own over time.

Third-party resiliency is best achieved through a combination of upfront agreements and ongoing arrangements that build resiliency between the engaging organization and the third party together.

Summary

As organizations mature their operational resiliency approaches, they must look holistically and proactively for ways to build resiliency into the fabric of the organization. Concepts like redundancy, diversification and adaptability are important. It is just as important to improve the BCMS program, ensure executive visibility, align resiliency and operational risk, and build a resilient third-party ecosystem. Taking action in these areas will significantly enable the organization to build operational resiliency.

Learn more about RSA Archer® solutions for business resiliency at rsa.com/irm.

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.