protiviti®
Face the Future with Confidence

Implementing Operational Resilience Across the Organization: An Essential Checklist

Like any enterprisewide organizational change, implementing an operational resilience program across an organization requires a careful and collaborative effort to be successful. Whether implementation has been in the works for several years or is just beginning, turning the resilience program from concept to reality is hard work.

Except for the most dynamic and change-oriented organizations, not all employees or managers will welcome the resilience program with open arms. Some resistance is natural, at least initially, given the potentially broad impact on culture (often entrenched at established institutions), cost, operations, roles and governance structure.

From the onset, the implementation team should be ready with a communication plan that concisely articulates the objectives of the change program and how those objectives will be measured. The executive leadership's expressed backing and expectations for firmwide collaboration should be emphasized in communications to employees.

In this paper, we explain many of the practical steps firms need to implement a resilience plan across the enterprise, using a checklist that details the practices, processes, systems and potential challenges business leaders should consider throughout the various phases.

The Resilience Implementation Checklist

As all firms are different, there is no single resilience checklist to make sure organizations are doing things properly. However, there are major items – critical considerations that, if ignored, would challenge implementation, and ultimately could derail the organization's chances of achieving its resilience goals. The considerations are discussed below:

Develop a Formal Resilience Strategy

Assuming the board has bought in to management's operational resilience goals, a formal strategy for embedding key resilience practices and processes into the organization should be developed and shared with the board for final consideration. The strategy should articulate the objectives of the program, timelines for implementation, and the basic questions of how the program will be governed and by whom.

While actual cost is important to understand, it is equally important to provide a budgetary justification for why the money should be spent and what the expected return would be. The argument may be summed up this way: The value of doing things right could mean a higher outlay in actual dollars; however, the increased cost should be measured against the consequences of not improving resilience.

Additionally, it should convey the key concepts of operational resilience, their particular applicability to the firm, and how the board and management can ensure success. Regulators' expectations of resilience across the industry and for the firm (particularly if there are recurring compliance issues) should be highlighted, along with the measures that are needed to mitigate those issues.

Finally, the strategy should include an analysis of the investment required for both the initial design and build-out, as well as to maintain the program. While actual cost is important to understand, it is equally important to provide a budgetary justification for why the money should be spent and what the expected return would be. The argument may be summed up this way: The value of doing things right could mean a higher outlay in actual dollars; however, the increased cost should be measured against the consequences of not improving resilience.

Create a Resilience Implementation Team (Champions of the Cause)

Now that the board has approved the formal resilience strategy, a cross-functional working group consisting of individual business service leaders should be created to lead implementation. As champions of the cause, these business leaders from across the organization will bring their understanding of the unique challenges and capabilities of the individual business units, ensuring that the efforts of the cross-functional group are applied consistently across the enterprise.

The team that will manage the resilience program going forward needs to be constituted. While there is no one-size-fits-all governance structure that works across all firms, we have found that centralizing a resilience team consisting of the senior leadership of business lines or services can yield significant benefits to many firms. The centralized office, led by a chief resilience officer, will serve as a knowledge hub, from where critical information would be collected and integrated into the resilience plan. This resilience office will ensure organizational consistency and alignment with the strategy.

In the case of one global bank, we discovered a resilience governance structure consisting of a chief resilience office, responsible for technology, business and cyber resilience, and a crisis management office, made up of a response team and a joint operations center. The members of the joint operations team were strategically located in key offices around the world.

Review Business Resilience Practices

With a team in place, it is time to begin the heavy lifting. It is worth noting that while many firms do not have a formal resilience program, the concept is not entirely new to them. In certain cases, a firm may find that about 85% of the practices and processes needed to be build resilience already exist through various other programs.

While some subjectivity will remain in any definition, internal, external and substitutability metrics are essential to assess a service's criticality to the institution, clients, the financial sector and the general public.

This means, in most cases, a review of current business resilience capabilities is necessary from the get-go. This process would include a full assessment of current business continuity management (BCM) and disaster-recovery (DR) programs. This enterprisewide assessment is necessary to enhance the team's understanding of how resilience differs across the organization and will inform how the resilience program is designed to enhance and extend current BCM and DR practices.

Identify Important Business Services and Processes

Beyond assessing current resilience capabilities, the team should begin the crucial work of developing a holistic view of all important business services and processes provided to customers, or, as U.S. federal bank regulatory agencies describe in a November 2020 paper, "critical operations" and "core business lines." Taking an end-to-end approach, this process involves assessing the criticality of people, technology, systems, third-party vendors and physical locations.

These regulators direct firms to identify their critical services and operations in their recovery or resolution plans (RRP) and to use the plans for managing and aligning their operational resilience to the most important services. This significant undertaking may require bringing in outside expertise to assist. A major challenge here is that for many global firms, business services and processes are not always contained within the institution or in a specific geographic area.

At this point, a common approach and framework may be needed to define important business services and processes and ensure global alignment. While some subjectivity will remain in any definition, internal, external and substitutability metrics are essential to assess a service's criticality to the institution, clients, the financial sector and the general public. The table provides sample metrics that can be considered to define service criticality at the firm level.

For processes, a front-to-back mapping approach allows the organization to identify specific processes and services as part of the effort to assess their importance or criticality. This detailed approach may include identifying the entry points for each process so that criticality can be determined from the view of the user. The front-to-back processes can be assessed at a higher level, or through different lenses such as volume, value, market share, reputational impact, systemic nature and substitutability.

For technology, a top-down risk assessment approach, usually conducted through one-on-one interviews or workshops with the senior management team, along with a review of policies or procedures and risk documentation, will provide a good indication of the big-ticket risk items that can bring down or harm mission-critical services, processes, systems and data.

	Metric Description	Metric	Details and Considerations
Internal Metrics	Percentage of overall revenue driven by business service	00.00%	If the business service is bifurcated from other business services, what is its share of overall revenue?
	Percentage of overall revenue supported by business service	00.00%	If a business service supports critical business services within the institution, what is its share of overall revenue?
	Estimated daily impact of business-service event to institution	$000,000.00	Daily cost to the institution based on the loss of revenue from the critical business service
	Estimated daily impact of business-service event to customers	$000,000.00	Daily cost to the institution's customers based on the loss of service from a critical business
	Difference of RTO versus impact resilience threshold	xx days	The difference between the time operations are restored and the impact threshold of the institution
External Metrics	Number of market participants providing business service	High/medium/low	Number of other institutions that provide a commensurate service
	Distribution of service among top market participants	High/medium/low	Distribution of market share among institutions that provide a commensurate service
	Regulatory exposure under outage of resilience event	High/medium/low	Anticipated regulatory response (fines and ongoing) of an event
	Regulatory expense under resilience event	$000,000.00	Anticipated regulatory cost (fines and ongoing) of an event
	RTO under resilience event	xx days	RTO
Substitutability of Services	Substitutability under resilience event	Yes/no	Under most scenarios, is the business service substitutable?
	Time to transfer service	xx days	Estimated delivery date for full-service transfer
	Transfer time vs. RTA (recovery time actual)	xx hours	Differential in transfer times vs. RTA
	Length of time service can operate under transfer scenario	xx days	If the business service can be substituted, what is the length of time of the transfer?

Measure Impact Tolerance/Tolerance for Disruption

This is the phase of the resilience-implementation process that involves creating a quantifiable method to determine the point in time when the viability of the identified important business services and processes is irrevocably threatened by an event. Regulators have proposed that firms express impact tolerance in a clear and sufficiently granular term so that it can be applied and tested. This can be a challenge if firms opt to use many common risk-quantification methods, which tend to express risks in ranges or with high-medium-low scoring.

The FAIR (Factor Analysis of Information Risk) methodology has proven to be an effective option to derive a financial representation of risk or loss exposure. Under the FAIR model, the primary factors that make up risk, such as loss-event frequency and loss magnitude, can be described mathematically, allowing firms to calculate risk from measurements and estimates of those risk factors. FAIR can be used to quantify different forms of loss, including productivity, response costs, replacement costs, and reputational damage. With this quantifiable output, management can take actions to take to remain within impact tolerance, including developing various time-critical triggering mechanism in advance to respond to disruptions as they occur and progress.

Embed Resilience Into the Culture

Now that you have a governance model and champions of the cause, and have identified your important business services and impact tolerance, what else is left to do? Your firm must continually drive the concepts of resilience until it becomes a component of its DNA. Everything from technology strategy to business-as-usual decisions should be evaluated with resilience as a key consideration and with a clear understanding of how the inability to deliver goods and services would harm all stakeholders, particularly customers.

How We Help Companies Succeed

Protiviti's financial services industry experts help organizations demonstrate and improve resilience through a robust testing program, building on existing business continuity management activities, IT disaster recovery and cybersecurity incident response. We work with and report to executive leaders and the board to address such questions as:

- Have we formally defined the important functions and services vital to the execution of the business model?
- Are impact tolerances established and tested?
- Are front-to-back mappings of components of the important functions and services understood and maintained?
- Is there a structure in place to govern resilience across the enterprise properly?
- Are extreme but plausible scenarios tested regularly?

Additionally, we partner with organizations to develop their overall operational resilience internal audit plans, incorporate operational resilience into existing audits and provide assurance over the operational resilience program. Click here to access Protiviti's operational resilience framework and additional thought leadership on the topic, including these related insights:

- Driving Operational Resilience From the C-Suite
- Operational Resilience Gets a Makeover in the 'New Normal'

Contacts

Ron Lefferts
Managing Director, Global Leader,
Protiviti Technology Consulting
+1.212.603.8317
ron.lefferts@protiviti.com

Kim Bozzella
Managing Director, Technology Consulting
Financial Services Industry Leader
+1.212.603.5429
kim.bozzella@protiviti.com

Andrew Retrum
Managing Director, Global Operational Resilience
Leader, Technology Consulting
+1.312.476.6353
andrew.retrum@protiviti.com

Thomas Lemon
Managing Director, UK Operational Resilience
Leader, Technology Consulting
+44.207.024.7526
thomas.lemon@protiviti.co.uk

Douglas Wilbert
Managing Director, US Operational Resilience
Leader, Risk & Compliance
+1.212.708.6399
douglas.wilbert@protiviti.com

Bernadine Reese
Managing Director, UK Operational Resilience
Leader, Risk & Compliance
+44.207.024.7589
bernadine.reese@protiviti.co.uk