

## Driving Operational Resilience From the C-Suite

The actions and decisions of C-suite leaders are typically driven by strategies designed to guide businesses toward growth and success. These plans invariably contain many assumptions. One is the expectation that their organizations will be able to deliver goods and services to customers even under stressful conditions – an expectation of resilience that is sometimes ill-conceived and unsupported.

Since the COVID-19 pandemic began, many business assumptions have been put to the test. C-suite leaders have been driving their organizations' crisis management, business continuity and operational resilience efforts. However, as the pandemic has shown, challenges to a firm's resilience are real, ever-changing and can easily extend beyond expectations in both severity and duration. Increasingly, boards are looking to the C-suite to build and demonstrate resilience, not with assumptions, but with meaningful and substantiated data. Forward-thinking leaders are not only going through the motions of how to move their businesses forward – keeping the lights on and keeping people employed – but also diligently tracking in real time what works and what does not work in order to make informed decisions that will enhance their resilience prospectively.

In this paper, we discuss key concepts and practices that C-suite leaders need to build operational resilience, the questions they should be asking, and the engagement required to assure all stakeholders that a resilience event can be effectively managed. We also address both the regulatory and market pressures firms must contend with to build resilience.

### Expectations of the C-suite

The causes of an operational disruption may be as simple as an equipment breakdown or as extreme as a pandemic like COVID-19. Either event may create the same consequence: the disruption of an organization's ability to deliver goods and services, thereby invalidating its business plans at the very least, or at worst, devolving its operations to the point where the organization is no longer a viable entity. Operational resilience is essentially the ability of firms (and a sector as a whole) to prevent, adapt to, respond to, and recover and learn from, operational disruptions.

Following are a few more important facts about the concept of resilience:

- Resilience is not just about or limited to business continuity management or disaster recovery, although both feed into it.
- Resilience expands and elevates existing business continuity and disaster recovery practices through more informed consideration of the impacts of severe-but-plausible events.
- For those organizations that are new to resilience, demonstrating an understanding of the issues may initially be more important than having the right answer.
- Resilience will continue to evolve. It is being examined by global regulators and will increasingly influence the decisions of the various key stakeholders that could be affected by a potential resilience event (i.e., consumers, investors, third-party suppliers, and the general public).

As key stakeholders' expectations of resilience continue to grow, organizations are under more pressure to assure their internal abilities, a directive that must come from the C-suite. Additionally, regulators are developing resilience rules that put the responsibility on C-suite leaders to set a tone from the top, meaning, champion resilience, foster a culture of resilience, and demonstrate that they understand the customer and market harm that a resilience event can cause. The tone-from-the-top expectation is also driven by regulators' view that without the active engagement of C-suite leaders, organizations cannot achieve their resilience goals.

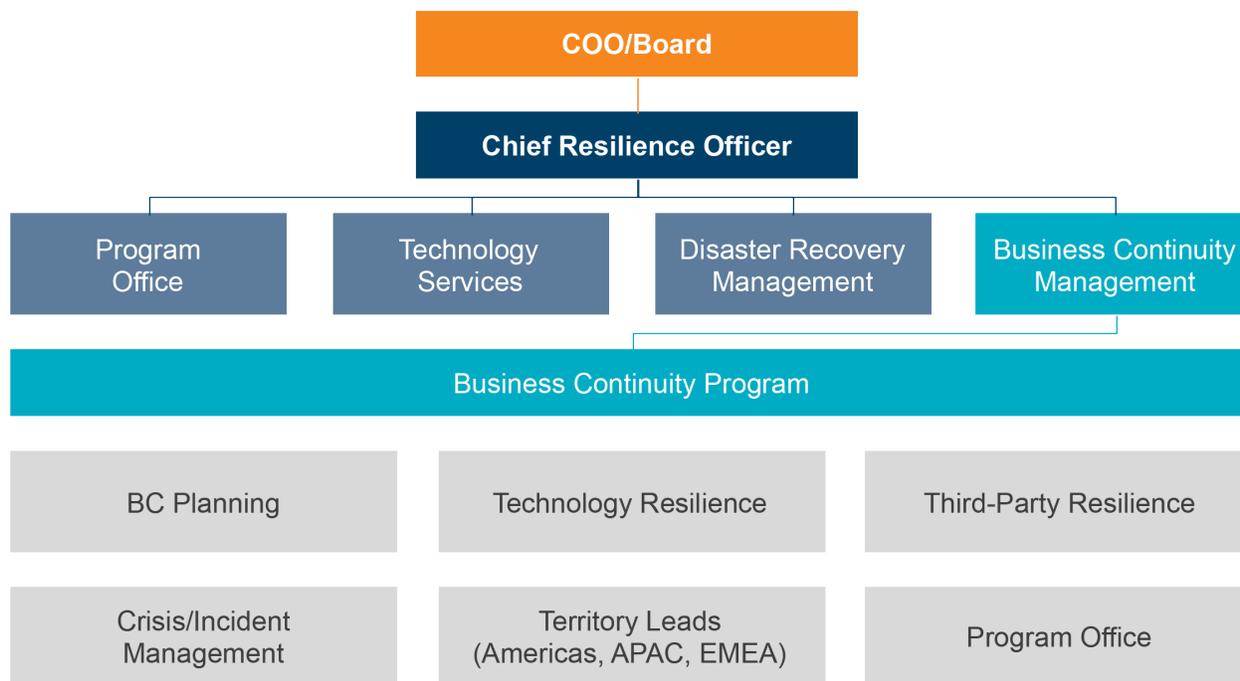
## **Resilience Measures and Functions**

What are some of the functional actions C-suite leaders can take to implement appropriate resilience? Or, most importantly, what are some of the factors that, if ignored, would increase the odds of failure in implementing an appropriate resilience program?

The following are some practical steps (and proposed rules) that C-suite leaders should consider:

### **Establishing a Head of Resilience or Resilience Office**

Given how broad and multifaceted resilience is, a senior role and/or an office can be created to manage, champion and report on a firm's resilience activities or programs. While the C-suite is expected to set the tone and provide guidance, and a second-line function can be designated to report on resilience, the cohesion an organization requires can be derived only from a function purposely designed to manage resilience. The illustration below shows a typical structure we have encountered at many large financial organizations:



### Reporting on Resilience

Do you have a clear understanding of your organization’s important business services and processes? Are you aware when systems go down? Do you know how long it would take to recover from a cyber event? Can you recover a business service quickly enough to meet your impact tolerance goals? These are just a few key questions around resilience that the C-suite needs to be able to answer.

The organization (the resilience office, to be precise) must be accountable to provide these answers on resilience to the C-suite, and the C-suite leaders should be prepared to challenge those assumptions as part of their responsibility to set the right tone and drive the overall corporate culture toward resilience. The resilience office and/or business lines should also provide regular reporting to the C-suite on levels of resilience in an ongoing effort to ensure accountability and drive cultural change.

To manage third-party related risks effectively, the C-suite is expected to provide the board with information on outsourcing that is clear, consistent, robust, timely, well-targeted and that contains an appropriate level of technical detail to facilitate effective oversight and challenge by the board.

### Quantifying Resilience

C-suite leaders are also expected to identify the important business services of the firm. At least one regulator has proposed that senior management (C-suite leaders) and the board should also set the impact tolerances (the maximum acceptable level of disruption) for each of the firm’s important business services. Quantifying downtime or measuring impact tolerance can come in many forms, but, at its core, it is a function of the cost of being down against a function of time.

Whether a firm is involved in payments processing or the clearing of security transactions, the basics remain the same: A firm can accept loss from an operational disruption for a specific period, after which it is bound to go out of business. The following are some key considerations for the C-suite when contemplating impact tolerance.

- Individual products or complementary services are often bundled, so an operational impact on one product may also affect multiple lines of business.
- Alternative services may be available for customers of a financial institution that are affected by a disruption.
- Cost decomposition is not just about lost revenue; regulatory fines and reputational damage should be factored in as well.

### Monitoring Resilience

A key aspect of understanding resilience risk is that it requires using discrete numbers to value the impact tolerance of the firm. Yellow, amber, and green charts should be replaced by functions that show the aggregate cost and decomposed costs of downtime. These figures will provide the C-suite a clearer picture of the resilience risk of the firm. Key performance indicators (KPIs) and key risk indicators (KRIs), metrics that firms have traditionally used to measure risk exposure, are useful only if C-suite leaders have a real-time understanding of the impact tolerances of their important business services.

Going forward, C-suite leaders should insist on resilience being a critical part of the organization's audit plan. In addition to specific activities that firms need to complete to demonstrate resilience, C-suite leaders should summarize their resilience activities in a written self-assessment, which, according to some regulators, would be provided upon request. A self-assessment is critical to advance the work efforts of the third line and provide regulators some comfort that the recoverability of a firm is acceptable.

Monitoring third-, fourth- and possible fifth- party risks and those beyond should be embedded in resilience activities to enhance recovery in the event of a supply chain-related disruption. Monitoring further down the supply chain and understanding where concentrations of services may exist downstream is critical, especially in the current environment, where many high-value services are spread among a small number of providers. Finally, the C-suite should contemplate both the reshoring and redundancy of services, as well as the cost factor needed to operate safely and effectively during a resilience event.

### Funding Your Resilience Program

How much does it cost to become resilient? C-suite leaders can expect this question from their boards. It is difficult to gauge the actual cost of becoming resilient, but it is not cheap. Beyond the cultural change needed to embed resilience in the minds of employees, there often needs to be technology change at the organization to enhance recovery. For instance, if a firm uses a private network with mainframes and end-of-life hardware, it may be a long and painful

process. On the other hand, for firms at the cutting edge of technology, like those employing cloud architecture with multiple redundancies, the cost of resilience may already be a part of a broader technology strategy, and therefore, already absorbed by the firm.

## **Taking Your Resilience Program to the Next Level**

A change in organizational culture will have the biggest impact on driving a firm's resilience. To foster this cultural change, the C-suite should embrace these key ideas:

- Be accepting of the financial burden needed to build resilience and recognize that the value of doing things right could mean a higher outlay in actual dollars. The increased cost, however, should be measured against the consequences of not improving resilience.
- Involve the entire organization in understanding, enhancing, and testing resilience. This inclusion is a primary driver of a cultural shift.
- Understand that the elephant in the room may not cause the most harm. For example, while the firm is mobilizing support for cybersecurity, do not ignore factors like end-of-life, change management and software updates.
- Key decisions around project selection, technology implementation and other key functions of the firm should consider how those decisions impact the firm's ability to recover from an event so that consumers are not harmed in the end.

Ultimately, for the C-suite, knowing where the organization stands on the resiliency scale is a primary step towards building an effective operational resilience program. This effort will inform how much work needs to be done (and obviously cost), and also increase the C-suite's understanding of the organization's resilience capabilities, thereby helping it to set appropriate expectations with regulators, the board, customers, employees and all stakeholders.

## How We Help Companies Succeed

Protiviti's financial services industry experts help organizations demonstrate and improve resilience through a robust testing program, building upon 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 and issues 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. Visit [here](#) to access Protiviti's operational resilience framework and thought leadership on the topic, including this recent insight: "[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](mailto:ron.lefferts@protiviti.com)

### Andrew Retrum

Managing Director, Global Operational Resilience  
Leader, Technology Consulting  
+1.312.476.6353  
[andrew.retrum@protiviti.com](mailto:andrew.retrum@protiviti.com)

### Douglas Wilbert

Managing Director, US Operational Resilience  
Leader, Risk & Compliance  
+1.212.708.6399  
[douglas.wilbert@protiviti.com](mailto:douglas.wilbert@protiviti.com)

### Kim Bozzella

Managing Director, Technology Consulting  
Financial Services Industry Leader  
+1.212.603.5429  
[kim.bozzella@protiviti.com](mailto:kim.bozzella@protiviti.com)

### Thomas Lemon

Managing Director, UK Operational Resilience  
Leader, Technology Consulting  
+44.207.024.7526  
[thomas.lemon@protiviti.co.uk](mailto:thomas.lemon@protiviti.co.uk)

### Bernadine Reese

Managing Director, UK Operational Resilience  
Leader, Risk & Compliance  
+44.207.024.7589  
[bernadine.reese@protiviti.co.uk](mailto:bernadine.reese@protiviti.co.uk)

---

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the [2020 Fortune 100 Best Companies to Work For](#)® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.