protiviti®

Face the Future with Confidence

Operational Resilience

Considerations for Boards, the C-Suite and Enterprisewide Implementation

Internal Audit, Risk, Business & Technology Consulting

Introduction

Since the beginning of 2020, organisations have been working tirelessly to address the range of complex issues accentuated by the COVID-19 pandemic. While this work continues for many organisations, forward-thinking business leaders are also looking beyond the crisis to operationalise new strategies that will help them build resilient enterprises for many decades to come.

Resilience is not about preventing operational outages or shocks but about how organisations prepare themselves to absorb events so they can recover quickly and continue to function or operate effectively. In a post-pandemic environment, technology will still create opportunities and vulnerabilities. Outsourcing to vendors and third-party contractors will provide efficiencies and reduce cost, but also create concentration and supply chain risks. The sophistication of cyber threats will continue to increase, and, surely, another ravaging pandemic in the not-so-distant future is no longer outside the realm of possibilities.

In consultation with operational risk experts and regulators around the world, Protiviti's thought leaders have been discussing and weighing the key considerations that should be top of mind for business leaders as they strategise over how to build resilience and thrive in a new and increasingly risky business environment. The insights developed from these engagements have been compiled in a series of white papers published over the past year.

In this report, we share several of the insights on operational resilience. The report includes a detailed discussion on the board's role in overseeing operational resilience and key considerations for directors; an analysis of the key concepts and practices that C-suite leaders need to understand to build operational resilience; and a checklist of practical steps firms need to implement a resilience plan across the enterprise.

Visit our Operational Resilience web site to access additional insights and our industry-leading operational resilience framework.

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 organisations 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 organisations' 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 organisation'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 organisation 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 organisations 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, organisations 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, organisations cannot achieve their resilience goals.

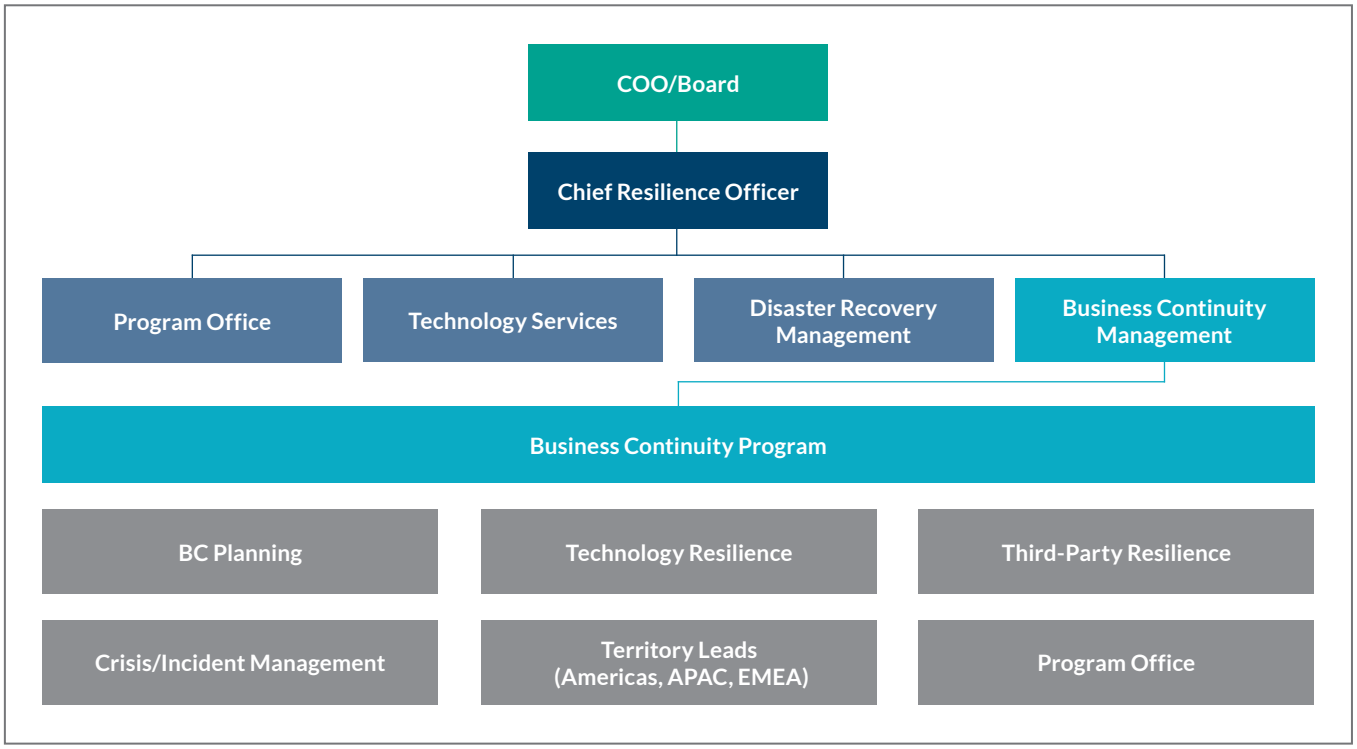
Resilience measures and functions

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 organisation 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 organisations:



Reporting on resilience

Do you have a clear understanding of your organisation'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 organisation (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 organisation's audit plan. In addition to specific activities that firms

need to complete to demonstrate resilience, C-suite leaders should summarise 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 organisation 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 organisational 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 recognise 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 organisation 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 mobilising 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 organisation 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 organisation'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 organisations 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 organisations to develop their overall operational resilience internal audit plans, incorporate operational resilience into existing audits, and provide assurance over the operational resilience program.

Operational resilience gets a makeover in the "new normal"

Churchill said he strived "to foretell what is going to happen tomorrow, next week, next month, and next year — and to have the ability afterwards to explain why it didn't happen." His acknowledgment of the futility in predicting the future is especially apropos today as markets transition to the eventual "new normal."

The business model is akin to a finely tuned machine requiring the coordination of multiple components to deliver value to customers according to a company's brand promise. Business models vary by industry. For example:

- A manufacturer's model combines a robust supply chain, an accessible labour pool, cutting-edge innovative processes, efficient facilities and equipment, and access to power, water and other necessary resources to produce quality products at competitive prices.
- A bank's business model might emphasise critical third-party providers, differentiating skills and competencies, and proprietary systems to enable superior customer experiences.
- An e-commerce retailer's model leverages supplier partnerships, efficient channels, world-class logistics and distinctive branding to offer a compelling value proposition to consumers.

Unless an organisation has an effective response plan, the absence or ineffective functioning of any of these components compromises the business model's viability. A loss of one or more components can take away the advantages of the model's underlying cost structure, the ability to produce or deliver products, and the capacity to provide essential services and/or accessibility to customers. Herein lies the crux of operational risk, or the risk that one or more scenarios impair the business model's effectiveness in fulfilling customer expectations and realising acceptable returns.

The COVID-19 pandemic has proven to be an object lesson on how severe this risk can be. Many were unprepared for an event that literally shut down major segments of the economy and even whole industries dependent on the gathering and concentration of people. Widespread failures of supply chains and third-party providers[1] and almost complete cessation of demand for products and services in some industries are unforgettable experiences that many might have regarded as implausible before the onset of the crisis.

The pandemic experience has served as a reminder that, in today's interconnected global marketplace, most companies are boundaryless due to their tight coupling with upstream suppliers and providers and downstream channels to reach ultimate end users. The concept of an extreme but plausible event becomes more pervasive when these dependencies extend, for example, as far upstream as third- and fourth-tier suppliers. Furthermore, the determination of "plausibility" when assessing extreme events continues to evolve as their frequency, severity, velocity and persistence increase.

But COVID-19 is just one example of a resilience event that stops the show. There are others, such as a cyberattack or catastrophic event. The velocity of such events varies. Whereas companies could see pandemic risk on the horizon charging toward them like a gray rhino, cyberattacks can occur suddenly and without warning.

[1] For example, a McKinsey survey of senior supply chain executives from across multiple industries and geographies indicated that 73% encountered problems in their supplier base, and 93% of respondents indicated that they plan to increase the level of resilience across their supply chain; see "Resetting Supply Chains for the Next Normal," July 21, 2020: www.mckinsey.com/business-functions/operations/our-insights/resetting-supply-chains-for-the-next-normal?cid=other-eml-alt-mip-mck&hlkid=fcba4c6a9dcc43a98273ecd1b4da4388&hctky=1368724&hdpid=3c3b6fa7-b102-490d-acd3-6380ab54b8e2.

As scenarios previously considered "implausible" were jolted into the "plausible" category — in effect, shifting probabilities assigned to tail-risk events closer to the mean — the question arises: What is the board's role in overseeing operational resilience post-pandemic? Below we offer several considerations for directors:

Learnings from the COVID-19 experience should drive advancements.

There has been much emphasis on continuous learning during the COVID-19 experience to understand what went well and what did not go well. The pandemic's severity offers powerful lessons for companies to consider and apply to facilitate an effective response plan should another pandemic or equally severe catastrophic scenario occur. Boards should encourage this review and request a summary of actions that management plans to take because of it.

Concentration risk warrants close attention.

While the term "concentration risk" is most often used in financial services to refer to exposures within a bank's asset portfolio arising from concentration to a single counterparty, sector or country, it also applies to other industries.

Geographic concentrations of critical assets, significant operational exposure to a geographically specific event (including sovereignty risk and regional conflicts), the concentration of information assets with outsourced functions, reliance on sole suppliers of critical raw materials and components, dependence on major customers for business, and other factors specific to a company's business model can create concentration risk.

For example, what if major customers were to fail, major customer contracts were not renewed, or major customers were to consolidate? Directors should be aware of these risks and, when they exist, ask management whether the specific concentration risk has been weighed against the cost and ability to recover within an appropriate time frame from an extreme but plausible event.

A virtual environment enhances resilience.

The pandemic has accelerated workplace redesign in most organisations. Companies able to virtualise their processes have been more successful during the pandemic lockdown than those unable or unwilling to do so. Going forward, there is an opportunity to reimagine work processes to ensure the highest form of resilience possible, which distributes the workforce, continues remote work arrangements, and supports a hybrid model that combines remote work with work physically performed in an office environment. The objective is twofold — accommodate the "new normal" workplace and contribute to increased operational resilience in facing catastrophic events that restrict workforce mobility.

Technology can be leveraged to increase resilience.

As noted above, companies able to operate their business virtually have provided an object lesson on the power of technology to facilitate resilience. Also, while most companies use the cloud, there are still quite a few that do not fully exploit its unique benefits. The cloud offers a scalable ecosystem, where damage to or the loss of operation of any single component of that ecosystem would not have a significant effect on the company's overall operations. Therefore, the cloud can contribute to the efficient deployment of the technologies that enable a virtual environment and improved operational resilience.

The right factors facilitate response readiness assessments.

Directors should ensure that management is asking the right questions when assessing exposure to extreme but plausible scenarios. The first is which critical business model functions, services and ecosystem components are most affected by the scenario? With respect to each scenario, what is:

- The velocity or speed to impact — that is, can the loss of key functions, services and ecosystem components occur without warning (e.g., a power outage)?
- The persistence of the impact, the duration of time before the loss of the functions, services and ecosystem components can be addressed, and the "headline effect" regarding the organisation's attempts to recover?
- The extent of the company's agility and readiness in responding to the event?
- The magnitude of uncompensated risks the company faces due to the loss of the component (e.g., loss of revenue stemming from downtime of services, permanent loss of customers, or the emergence of health and safety issues)?

The likelihood of occurrence is not a prime consideration in this assessment. The focus is on what management will do when the event occurs.

Operational resilience intersects risk and crisis management.

Every director and CEO faces the spectre that, no matter what they do, there will always be the possibility of an unforeseen disruptive crisis occurring for which there is no playbook available.

But this reality should not stifle efforts to plan and prepare for disruptions. Just as a crisis is a severe manifestation of risk, crisis management is the natural follow-on to risk management.

Rapid response to sudden, unexpected events depends on the enterprise's preparedness and response plans. Building a reliable crisis management capability is a management imperative for scenarios with a high-reputation impact and velocity. A world-class response to a persistent crisis is vital to the company's ultimate recovery and preservation of its brand image. Operational resilience assessments focused on the factors mentioned above can help identify areas where preparedness is more critical.

The board needs to be more focused on resilience.

Now that we've experienced the worst pandemic in a century, directors should pay more attention to operational resilience going forward. With disruptive change the norm, it is necessary to be agile and adaptive.

The board should understand and offer input on the operational resilience strategy, including the identification of functions, services and ecosystem partners defined as critical to the execution of the business model. The board should request that it be notified promptly when an event occurs that is likely to require public or regulatory disclosure or that meets specified criteria — for example, "close calls" such as a nearby hurricane or an attempted cyberattack that could have adversely affected an important business function or service. When reportable events are brought to the board's attention, directors should also understand and advise on management's strategy for improving resilience.

There are different views as to how granular the board's focus on operational matters should be. But there should be general agreement as to the organisation's targeted recovery time for an important business service or process that guides the assessment of resilience plans. Directors should also gain confidence in the company's operational resilience team and with their line of sight into the team's activities.

Operational resilience is a strategic imperative. Directors should inquire about the scope of resilience planning at the companies they serve to ensure that it encompasses an end-to-end extended enterprise view of the value chain that looks upstream to suppliers and third-party providers, and downstream to channels and customer relationships. These business ecosystem partnerial relationships are just as crucial to the business model's execution as the organisation's internal processes, personnel and systems. Evaluation of operational threats, therefore, should be directed toward understanding the company's resilience in addressing any of these key links in the chain and whether the time frame to recover is acceptable in sustaining the operation of the business model.

This comprehensive view is important. According to Gartner, business continuity management and organisational resilience programs are not keeping up with digital transformation initiatives and emerging, more complex threats.[2] These programs should be a business-as-usual activity inextricably tied to the achievement of corporate objectives, customer fulfillment commitments, and expressed or implied brand promises. A comprehensive view of all key components of the business model is needed to create that linkage.

The operative question is: What would happen to the organisation's ability to execute its business model if any of the model's underlying components are taken away through an unexpected catastrophic event or altered in such a significant way as to place the company at a strategic disadvantage? Said another way, at every stage of the value creation process, what would be the implications of a shortage, disruption or quality problem in an input or output? In such scenarios, how long would the company be able to operate? This pervasive question applies to such inputs as the available labour force and talent pool, the availability of power at a reasonable price, and the availability of lines of credit and working capital. This kind of thinking is needed in a disruptive world.

In considering these boardroom discussions, directors should be kept up to date on business continuity regulatory requirements and standards specific to the sector(s) in which the company operates, as well as the efficacy of management's processes for complying with them. These regulations and standards often provide guidance on required or suggested areas of focus and approaches. The most comprehensive guidelines and standards are geared toward financial services. Using these more rigorous guidelines, it is not uncommon for other industries to apply the strategies and controls that are most relevant, as they offer a best practices model.

[2] "2020 Strategic Road Map for Business Continuity Management," Gartner, February 21, 2020, available at www.gartner.com/doc/reprints?id=1-1YL4N1MD&ct=200311&st=sb.

Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Does the board have sufficient transparency into management's definition of the business functions, services and ecosystem partners critical to the execution of the business model?
- Do directors understand management's process for determining the impact tolerances on important functions, services and ecosystem partners (i.e., how long can the company operate without them)? Does management consider extreme but plausible events that could result in an impact on the business that exceeds established tolerances?
- Is the board informed promptly of events that have occurred that either require disclosure or meet its specified criteria for timely notification?
- How prepared is the organisation for operational resilience? Has management implemented reliable processes, systems, metrics and response plans to ensure organisational preparedness? Is the organisation conducting periodic tabletop exercises that effectively test its ability to recover against extreme but plausible scenarios? How does the board know?

How Protiviti can help

We partner with organisations to develop overall operational resilience internal audit plans, incorporate operational resilience into existing audits, and provide assurance over the operational resilience program. We work with and report to executive leaders and the board, as directed, 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?

We help organisations demonstrate and improve resilience through a robust testing program, building upon existing business continuity management activities, IT disaster recovery and cybersecurity incident response.

Implementing operational resilience across the organisation: An essential checklist

Like any enterprisewide organisational change, implementing an operational resilience program across an organisation 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 organisations, 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 emphasised 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 organisations are doing things properly. However, there are major items — critical considerations that, if ignored, would challenge implementation, and ultimately could derail the organisation'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 organisation 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.

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.

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 organisation 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 centralising a resilience team consisting of the senior leadership of business lines or services can yield significant benefits to many firms. The centralised 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 organisational 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 centre. 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.

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 organisation 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.

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.

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 organisation 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.

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

	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?

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 organisations 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 organisations to develop their overall operational resilience internal audit plans, incorporate operational resilience into existing audits and provide assurance over the operational resilience program.

ABOUT PROTIVITI

Protiviti (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.

CONTACTS

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

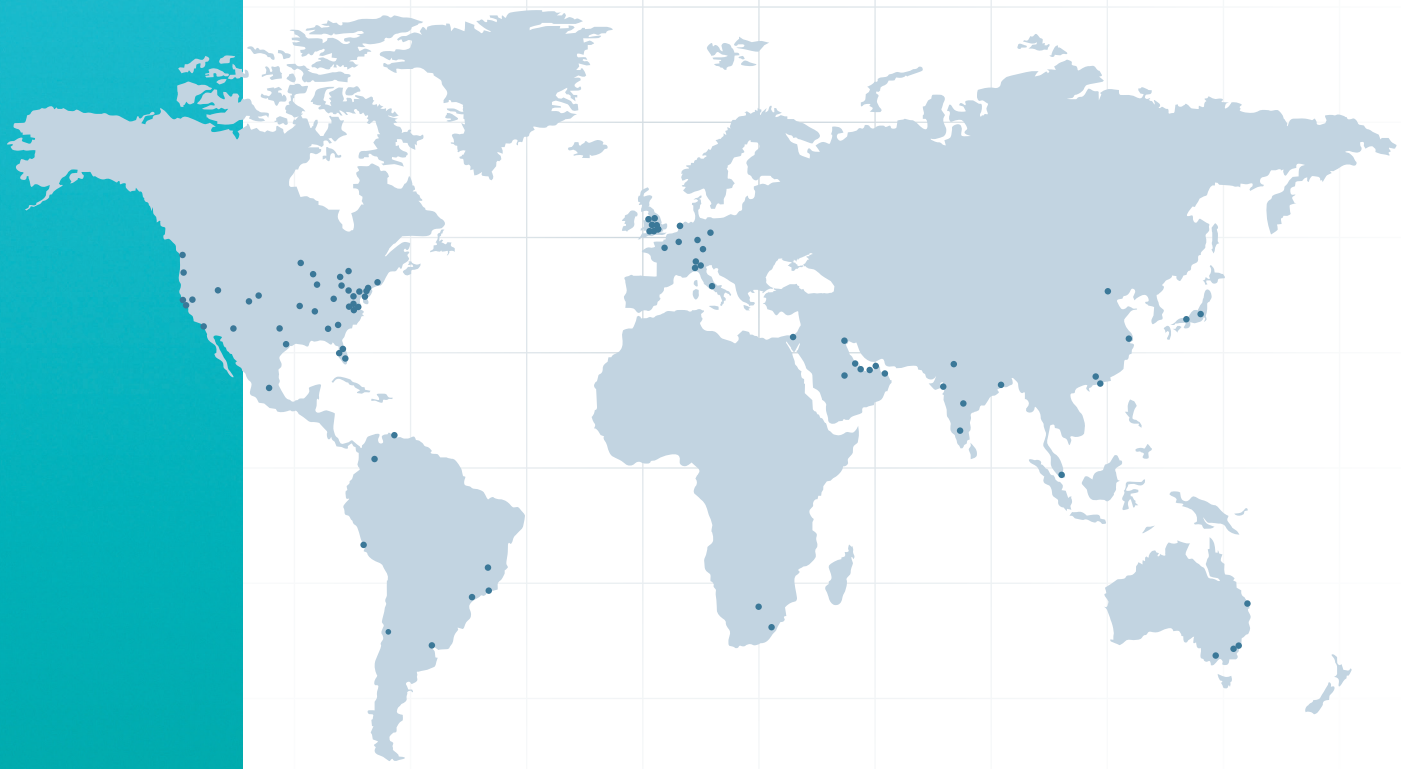
Douglas Wilbert
Managing Director,
US Operational Resilience Leader,
Risk & Compliance
+1.212.708.6399
douglas.wilbert@protiviti.com

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

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

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

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



THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®