IDC
Analyze the Future

WHITE PAPER

Lack of Operational Resilience Will Undermine Enterprise Competitiveness: A Strategy for Availability

Sponsored by: SunGard Availability Services

David Tapper
April 2013

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

EXECUTIVE SUMMARY

What do the following events have in common: cyberattacks, severe weather, health pandemics, and power outages? They all drive organizations to develop a very sophisticated means of "availability" — maintaining uninterrupted business operations. The key to success is building availability processes for operational resilience that integrate, orchestrate, and align the priorities and objectives of line-of-business (LOB) executives, such as CXOs and VPs/managers of business processes, with those of IT.

Why? Because disasters, natural or man made, can potentially cripple or halt an organization's business objectives, from ensuring growth targets and brand equity to optimizing supply chains and worker productivity. Organizations must be always available and able to manage these events in a way that works with their traditional stakeholders of internal business units, supply chains, business partners, and manufacturing. But also, and more importantly, the approach must work with customers — and even governments, the media, and investors.

To achieve comprehensive, continuous availability, whether for daily goals or unexpected events, organizations must implement a new paradigm of operational resilience. The best definition of operational resilience is "an emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption" (source: Carnegie Mellon's Resilience Management Model CERT-RMM). This requires three key availability building blocks: information security and data governance, business continuity/disaster recovery, and IT service management. Collectively, these three disciplines support the level of agility and resilience needed for an enterprise to maintain "always available" operations.

To gain an enterprise view of operational resilience, and how prepared enterprises are in providing such capabilities, IDC interviewed more than 900 LOB and IT executives in the United States and United Kingdom across a series of industries. Based on these interviews and subsequent analysis, IDC has identified the following four key findings:

- **Expectations of operational resilience are very high.** The combined view of LOB and IT highlights that the top criteria for operational resilience should cover several capabilities. These include the need for an always-on business and IT environment that can make changes quickly to existing business processes and the ability to manage disruptions, provision new services quickly, and minimize costs via a pay-as-you-go consumption model. Consequently, organizations will need to develop a holistic set of capabilities to support this breadth of requirements.

- **Significant vulnerabilities exist in achieving operational resilience.** This document reveals that organizations have some fundamental problems that will hinder their ability to achieve this level of operational resilience. This happens through a combination of insufficient capabilities (e.g., risk management, security, business continuity) and potential structural misalignments between LOB and IT objectives, as well as between enterprise focus and market needs.

- **Vulnerabilities could result in enterprise underperformance.** These vulnerabilities could lead to significant underperformance by an enterprise. This could involve not meeting key financial objectives (e.g., sales targets, product introduction, growth, margins) and/or IT service delivery requirements (e.g., availability, recoverability, speed of provisioning, scalability).

- **Enterprises need to develop a strategy for ensuring operational resilience.** To achieve operational resilience, enterprises need to develop a strategy that involves developing leading key performance indicators (KPIs), performing a gap analysis, implementing strategic change initiatives, creating a holistic enterprisewide governance structure, and incorporating an optimal sourcing model.

The study results provide enterprises with a set of benchmarks for implementing an effective operational resilience program. These benchmarks can also provide organizations with peer assessment tools for understanding their relative competitive capabilities when it comes to operational resilience by industry, geography, or company size. Additionally, this study furnishes a road map for achieving the level of operational resilience needed to maintain continuous business operations in the face of rapid market shifts and natural disaster events such as fires and floods.

PERCEPTION OF OPERATIONAL RESILIENCE: SETTING A NEW BAR

The bar for operational resilience is set very high. Figure 1 provides feedback of what both LOB and IT view as key characteristics of operational resilience. Significant factors characterizing the IT view of operational resilience are focused more on business and IT services that are "always on" and available, as indicated by 37% of IT respondents, followed by 18% highlighting the ability to respond to and minimize the impact of events that disrupt operations.

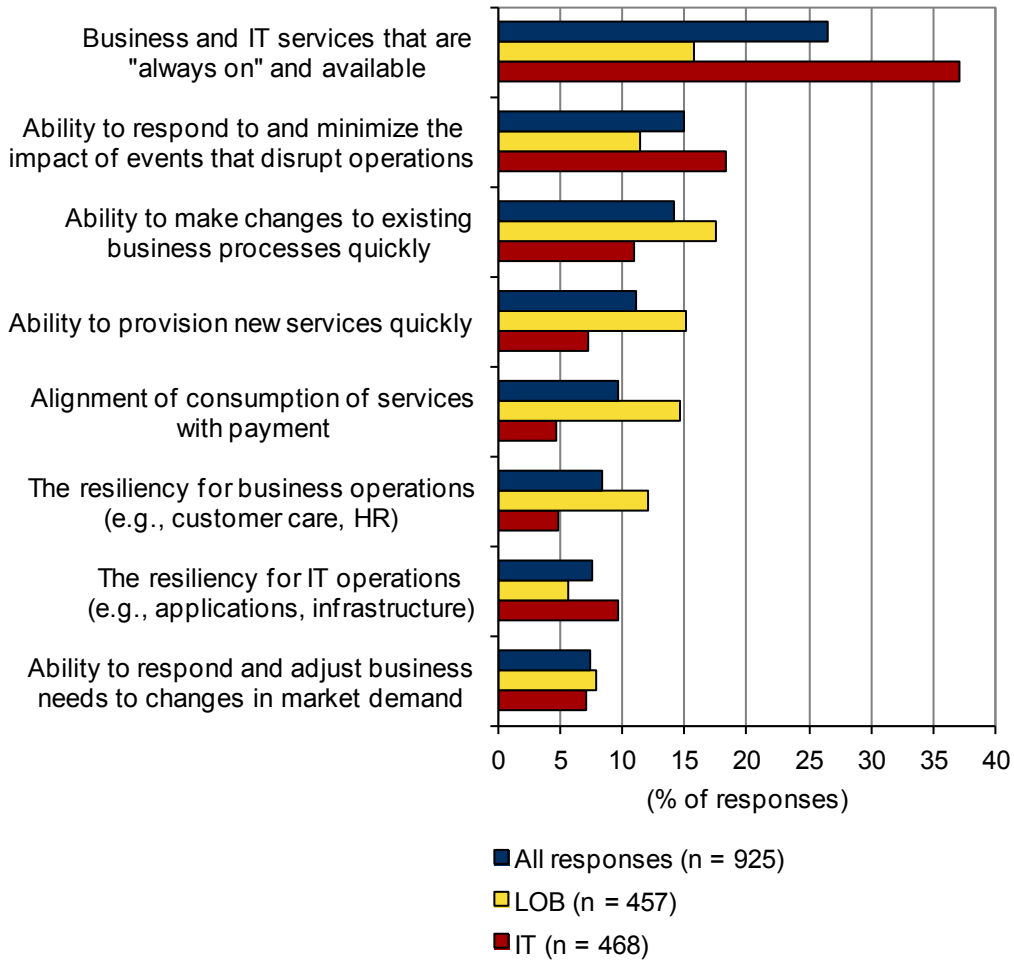
In contrast, LOB's view of operational resilience appears to be much broader, with 15–18% of these respondents including the top characteristic selected by IT (always on) plus the ability of operational resilience to make changes to existing business processes quickly, to provision new services quickly, and to support alignment of consumption of services with payment. However, and more importantly, when combined, the views of operational resilience by LOB and IT highlight the breadth of capability an organization needs to guarantee continued business operations under any conditions.

The level of stringent requirements is also reflected by 90% of LOB and IT respondents indicating their expectation of one day or less of downtime annually, which translates to 99.7% uptime or greater. When coupled with the accelerating pace of change, enterprise expectations for a wide-ranging set of service levels, including contracted service-level agreements (SLAs), will also become more acute (e.g., speed of provisioning, scalability, recovery time).

FIGURE 1

Enterprise Perception of Operational Resilience

Q. Which statement best represents your organization's concept of "operational resilience"?



Source: IDC, 2012

TOP ENTERPRISE PRIORITIES AND STRATEGIC CONCERNS

Ensuring competitiveness for enterprises involves addressing some key priorities and strategic concerns. Based on feedback from the nearly 1,000 respondents in this study, these factors span dealing with strategic risks, ensuring the ability to optimize ROI, and effectively managing key IT objectives. However, it is critical for enterprises to recognize that while there is common ground between LOB and IT across these factors that can help achieve the required operational resilience, there are some crucial differences between these two key stakeholders. LOB has a more external focus (e.g., markets), and IT has an internal focus (e.g., IT operations). The resulting tension between these two groups caused by these differences will likely inhibit achieving the level of operational resilience needed to compete effectively. In detail:

- **Strategic risks.** Both LOB and IT agree that increasing operational costs, external compliance with government/regulatory pressures, and supporting customers and/or business partners in their compliance requirements are paramount challenges that enterprises face in managing risks. However, while LOB considers business complexity and market pressures as additional risks to ensuring competitiveness, IT lists rapid introduction of new technology and loss of people as some of its top risks.

- **Challenges in executing corporate strategy.** All respondents agree that the greatest challenges across the enterprise involve the ability to focus the right people and resources on strategic initiatives while aligning business with IT. But LOB indicates some key additional factors including the need to meet demands for growth and increased revenue, to compensate for economic factors, and to increase introductions of new products and services.

- **IT operation imperatives.** Topping IT operation imperatives for both LOB and IT are the need to improve IT operation service-level performance and the need to achieve cost-reduction goals. However, LOB views include improving supply chains as an additional operational imperative, while IT highlights improving technology architectural resiliency.

- **Financial management.** Companies indicate that financial integration and eliminating financial silos are major challenges. IT highlights pressure to drive down IT maintenance/support costs. LOB ranks market forecasts, risk identification and impact mitigation, and current market/business conditions as top influencers for budgeting and financial management.

- **Changes in technology and service delivery.** Factors involving technology and service delivery are driven primarily by IT, such as improving technology architecture resiliency while managing rapid changes in technology more effectively. Additional factors include the need to transform/modernize internal IT environments to "mimic" that of a cloud model and reduce complexity/consolidate systems/applications while increasing the use of automation across IT systems.

ARE ENTERPRISES PREPARED?

IDC believes that the level of operational resilience needed to ensure competitiveness will require prioritizing, synchronizing, and orchestrating a vast set of factors and resources across an enterprise. These must include the three key building blocks of an operational resilience business model — security, business continuity/disaster recovery, and IT service management. The discussion in the Top Enterprise Priorities and Strategic Concerns section provides a window into some of the differences in priorities between LOB and IT that can hinder the ability of organizations to achieve operational resilience, but IDC has also identified additional strategic areas that could further impede enterprises from attaining these goals.

Insufficient Capabilities

Insufficient capabilities involve factors required to orchestrate operational resilience (e.g., risk management) or critical building blocks of operational resilience (e.g., security, business continuity). Both LOB and IT agree that their organizations show significant weaknesses in these areas:

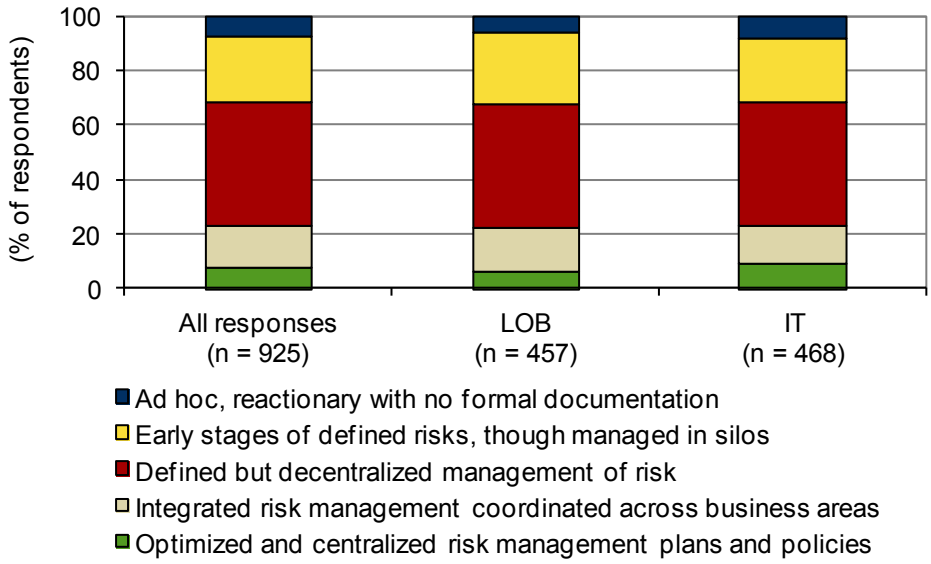
- **Risk management structure:** Figure 2 highlights an enterprise view of risk management, with 77% of respondents indicating that they have a more "decentralized" risk management capability. This lack of a centralized risk management function can easily undermine the ability of an organization to coordinate the right response to rapid market changes and shifts.

- **Ability to respond to security breaches and business operation failures:** Figure 3 highlights the belief that enterprises lack the right capabilities to respond effectively to security breaches or potential business operation failures, with a ranking of just 2+ out of 5 for both areas. Respondents also selected security as the area of most concern when ranking the potential impact of key events on continuous business operations, followed by compliance violation and supply chain failure. Further, Figure 4 shows that top security requirements for ensuring operational resilience must involve knowledge of particular industry needs as well as the ability to comply with regulations and other industry codes. Deficiencies in these areas will keep organizations from responding to significant security breaches and business operation failures effectively.

FIGURE 2

Enterprise Risk Management Level of Maturity

Q. How formal/mature is risk management at your organization?

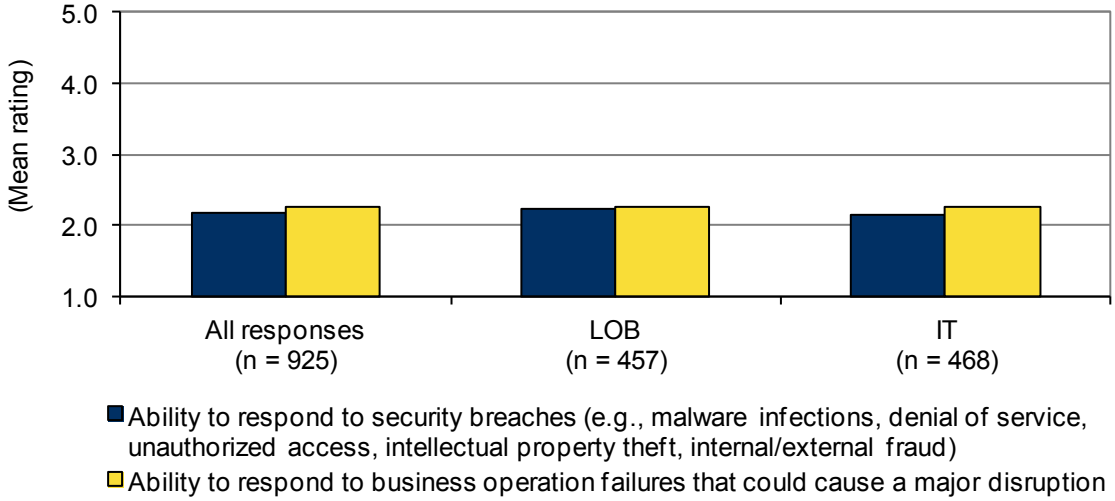


Source: IDC, 2012

FIGURE 3

Ability to Respond to Security Breaches and Business Operation Failures

Q. Rank your ability to respond to security breaches and ability to respond to business operation failures that could cause a major disruption.



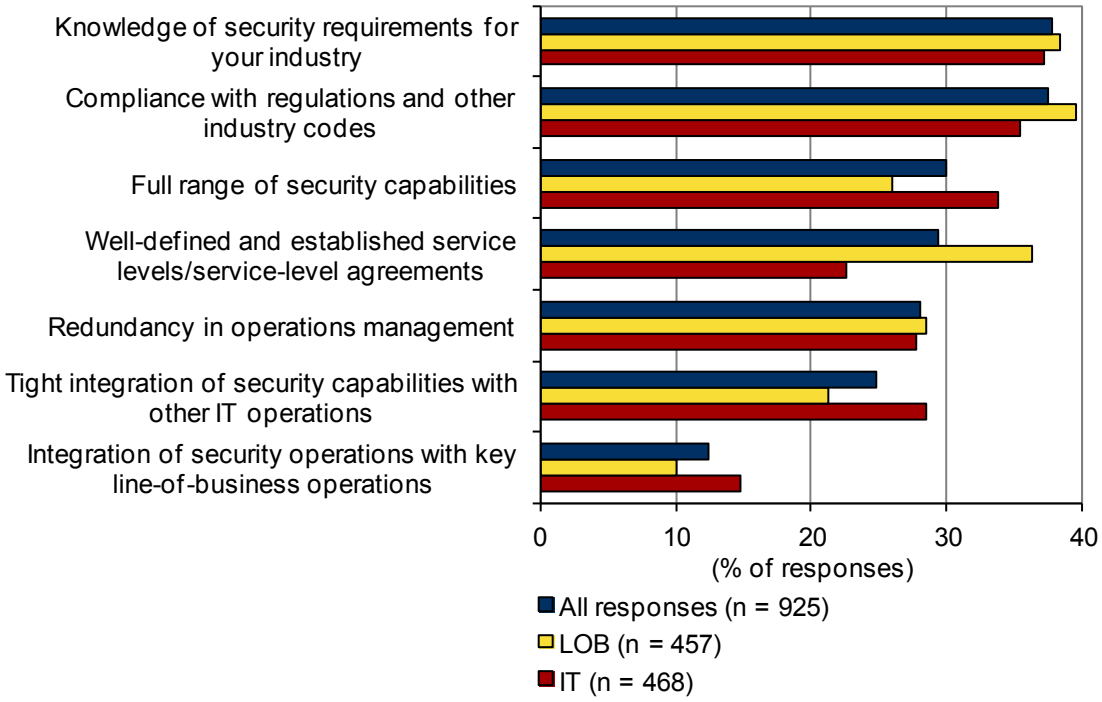
Note: 5 = extremely good (e.g., little to no disruption of operations, no financial loss or liabilities, no brand or reputational damage), 3 = moderate (e.g., some loss of business revenue, operational functionality, brand value), and 1 = very poor (e.g., major financial losses, considerable impact on operational functions, brand value diminished)

Source: IDC, 2012

FIGURE 4

Top Security Factors for Ensuring Operational Resilience

Q. Select the top 2 security areas that are critical to ensuring operational resilience.



Source: IDC, 2012

Structural Misalignments

Structural misalignments involve "gaps" between LOB and IT stakeholders and between enterprise priorities and market demands. These vary from the structure of the organization and business continuity priorities to speed of service provisioning requirements and changing customer interactions.

LOB Versus IT

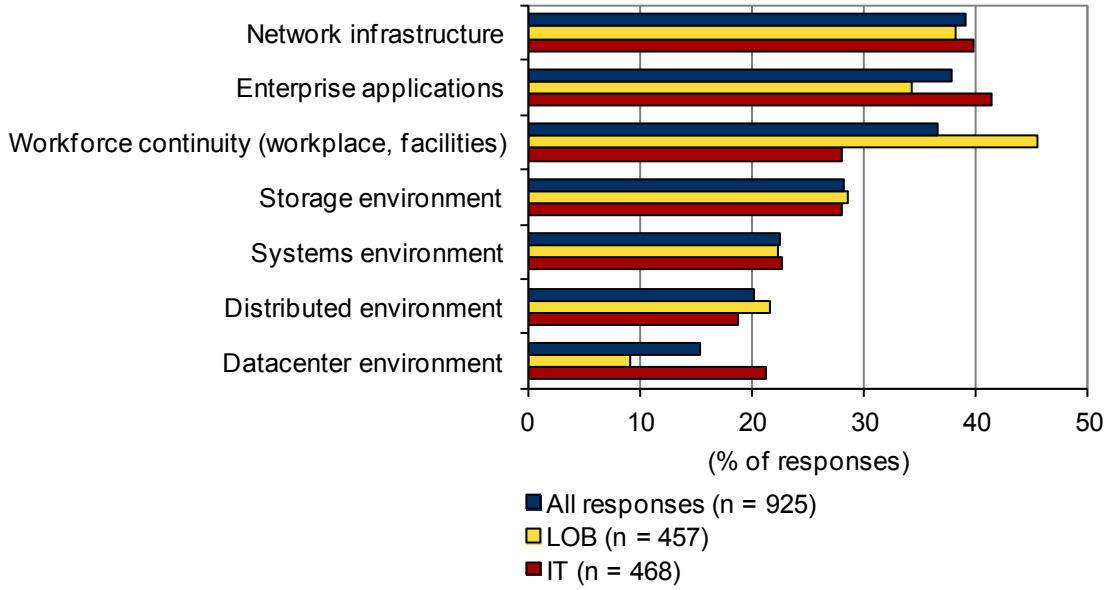
- **Operational resilience expectations.** When it comes to expectations of operational resilience, LOB indicates a broader set of priorities than IT. While both look for an "always on" environment, additional LOB factors include the ability to make changes quickly to existing business processes, provision new services quickly, and minimize costs via a pay-as-you-go consumption model. A successful operational resilience strategy needs to combine both IT and LOB needs.
- **Organizational structures.** LOB indicates that it is more decentralized, while IT is more centralized. The challenge for an organization today is to guarantee that all its business units, even if more federated, can support common areas across the enterprise, particularly functions such as overall brand, common processes (e.g., supply chain, marketing, sales), and investments (e.g., infrastructure, partnerships), to name a few. Any lack of organizational alignment between IT and LOB can only further undermine business performance.

- **Business continuity priorities.** As Figure 5 shows, LOB ranked workforce continuity as its top focus in ensuring availability, while IT selected enterprise applications. These different priorities will limit an organization's ability to synchronize and orchestrate all resources needed to achieve operational resilience.

FIGURE 5

Top Priorities for Ensuring Availability

Q. To ensure availability of your business processes, select the two areas that require the greatest focus in the next 12 months.



Source: IDC, 2012

Enterprise Versus the Market

IDC has also identified the following two areas for which organizations may be fundamentally misaligned with the market. These will only further complicate the ability of enterprises to meet the required level of agility and operational resilience. In detail:

- **Ensuring speed to market.** LOB indicates that speed of provisioning new services is critical to operational resilience. However, IT indicates that the frequency of provisioning application functionality, on average, is no more than quarterly. IDC believes that IT will need to accelerate this speed considerably, particularly as cloud becomes a larger part of service provisioning. IDC studies indicate that some of the market already expects provisioning of an application within a day when using cloud services.
- **Customer relationship interactions.** The results of this study show that, on average, about 11% of customer interactions are technology based versus direct sales. IDC believes that this will have to change fairly quickly, as reflected by the rapid shift in customer care services from using voice-based interactions to a Web-centric, technology-centric approach (e.g., Web, click to chat, social media).

Unique Differences by Key Segments

While there are a broad set of factors impacting the ability of organizations to achieve the level of operational resilience that they need to ensure competitiveness, not all organizations will have the same issues. Many of these issues will depend on the market segment in which an enterprise competes, whether by size of company, geographic location, and/or industry. Figure 6 provides a snapshot of just a few of these differences in comparing organizations within each of these segments. Identifying an organization's insufficient capabilities or structural misalignments by these segments will help determine unique characteristics and how to address them.

FIGURE 6

Key Market Segment Differences by Geography, Company Size, and Industry

Geographies: United States versus United Kingdom	**Risk Management Maturity**	▪ **United Kingdom:** Risk management level slightly better than United States
	Availability Requirements	▪ **United States:** Slightly higher level for LOB and IT availability expectations
	Factors Impacting Risk	▪ **United Kingdom:** Business complexity and uncontrollable events ▪ **United States:** New technologies and compliance with ▪ customers-partners
Size of firms	**Risk Management Maturity**	▪ **Larger firms:** More integrated and optimized
	Availability Requirements	▪ **Smaller firms:** IT availability requirements higher ▪ **Larger firms:** LOB availability requirements higher
	Security Breaches	▪ **Larger firms:** Higher frequency of security breaches
Industries	**Risk Management Maturity**	▪ **Financial Services:** Risk management more well defined ▪ **Healthcare:** Less well-defined risk management
	IT Operational Imperatives	▪ **Retail-wholesale:** Reduce application downtime ▪ **Professional services:** Migrate to virtualized or cloud model

Source: IDC, 2012

RECOMMENDATIONS

The pressure for enterprises to perform has never been greater, whether that means achieving improved financials, better brand management, operational efficiencies, product innovation, and global expansion or increasing worker productivity. A key element to enabling all these is creating an organization with the level of availability, operational resilience, and agility needed to maintain its competitiveness and continuous business operations. However, the results of this study highlight that organizations are underprepared to do this, and that success in achieving the right level of operational resilience will require organizations to do the following:

- **Develop KPIs, a risk profile, and a blueprint for operational resilience.** Organizations need to define their level of operational resilience via targeted leading KPIs across business factors (e.g., customer support, sales) and IT services capability (e.g., availability, RPO, speed of service provisioning). Organizations should also create a comprehensive risk profile that incorporates all critical factors both internally and externally that will impact these KPIs. Finally, organizations can use the KPIs and the risk profile to create a blueprint of business and IT objectives and the associated people, technologies, and processes required for the level of operational resilience required.

- **Perform gap analysis.** After developing the combination of established KPIs, a risk profile, and a blueprint, organizations then need to perform a gap analysis of their business(es) to identify areas of strength and weakness based on the capabilities required to achieve the right level of operational resilience. This gap analysis must assess the alignment (or lack thereof) between LOB and IT objectives as well as the alignment of enterprise priorities with market needs to help further identify areas to address.

- **Implement strategic change initiatives.** By utilizing results of a gap analysis, organizations should focus on the areas needing improvement or potentially strategic realignment and investment. Organizations may want to select two or three established gaps to focus on initially and define specific criteria to select these areas, such as strategic KPIs, strategic risks, specific business processes, industry requirements, or target markets. Success achieved in these select areas can then be used to pursue larger initiatives.

- **Develop a holistic enterprisewide governance and risk management system.** Organizations need to build an enterprisewide governance system that can manage all the key components (business and IT) impacting the required level of operational resilience. This system ultimately will need to incorporate all of the organization's people, processes, and technological capabilities, as well as include external stakeholders such as supply chains, business partners, service providers, and customers and those that could have additional strategic influence on the organization (e.g., media, governments, investors).

- **Incorporate an optimal "sourcing" model for operational resilience.** Achieving the level of operational resilience needed to compete effectively will require organizations to develop an optimal "sourcing" model that incorporates in-house resources and outsourced resources, with particular focus on managing across traditional services (e.g., more labor-based services model) and cloud services (e.g., more highly automated). Outsourcing can potentially help provide additional expertise and economies of scale to fill gaps or strengthen vulnerabilities while also achieving cost efficiencies such as lowering overall costs and shifting budget from capex to opex.

  Overall, the objective is to ensure that an organization has all the resources it needs to achieve its KPIs and mitigate its risks while ensuring operational resilience and agility.