Gartner Research

Manage Risk in Crisis-Driven Decisions From Response Through Recovery

By Paul Proctor, Srinath Sampath

28 February 2022

Gartner®

Manage Risk in Crisis-Driven Decisions From Response Through Recovery

Published 28 February 2022 - ID G00767454 - 15 min read

By Analyst(s): Paul Proctor, Srinath Sampath

Initiatives: Executive Leadership: Strategic Risk Management; Executive Leadership: Strategic Cost Optimization

> Disruptions such as the Russian invasion of Ukraine are times of heightened uncertainty, placing an additional premium on risk-based decision making. Executive leaders who make defensible, risk-informed choices are more likely to navigate their organizations with resilience, from response through recovery.

Overview

Key Findings

- Executive leaders may be used to making risk-informed decisions, but crises such as the Russian invasion of Ukraine challenge the usual playbook.
- Crises have a mix of characteristics — time crunch, loss of control and heightened uncertainty — that increase the difficulty and importance of risk-informed decision making.
- Depending on the root causes and consequences of a crisis, the risk profile of the organization can change very extensively and very rapidly.
- Spending cuts may be inevitable, and these choices may decrease risk in one area while exacerbating other risk exposures.

Recommendations

Executive leaders focused on IT cost optimization, finance, risk and value should:

- Critically analyze the current and future effects their decisions could have on the organization's overall risk exposure by assessing the risk interdependencies that exist in all phases of the crisis.

- Build defensibility in the eyes of key stakeholders by creating an institutional record of crisis-time decisions as well as the dependencies considered and the risks accepted.
- Build plans to manage key dependencies, where possible, if the downside risk is unacceptable or if it presents an opportunity that can be leveraged for organizational benefit.
- Identify metrics that can help the organization track the status of key dependencies to manage any excessive downstream effects.

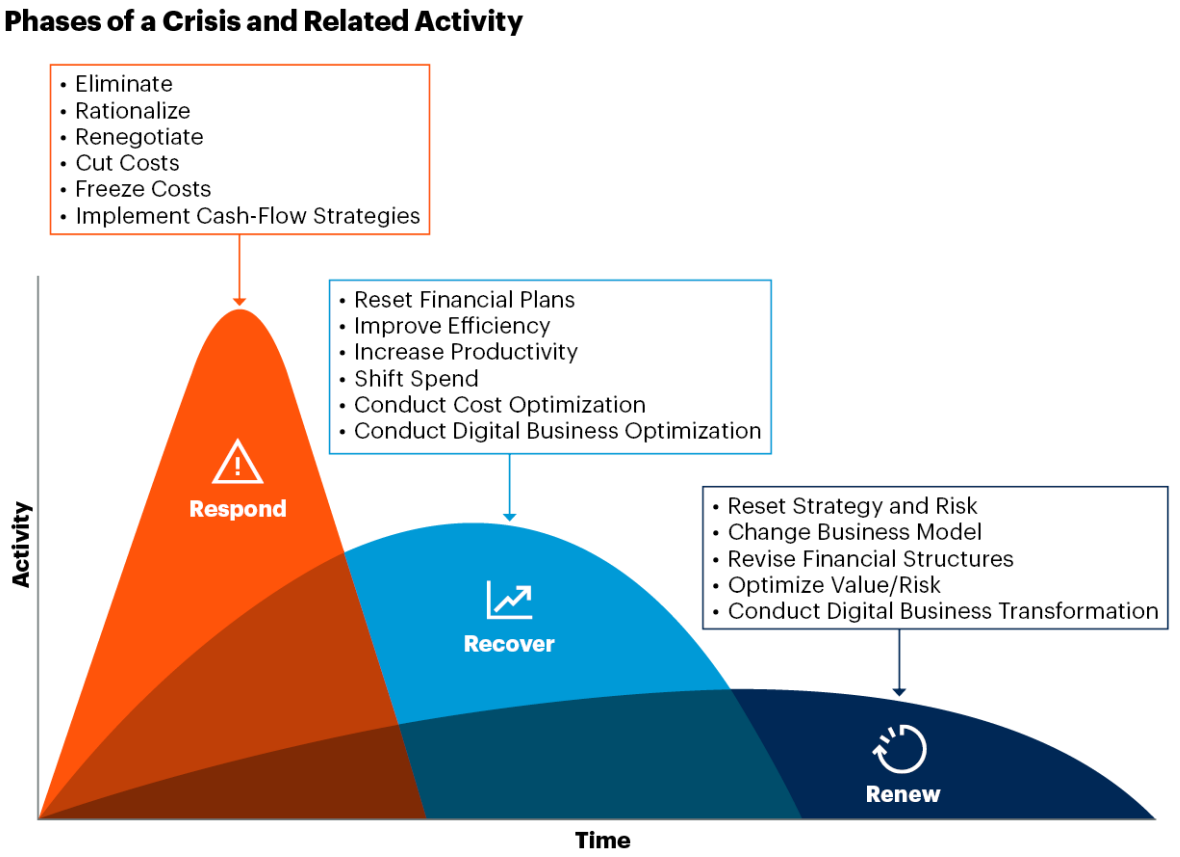
Introduction

Good risk management is informed decision making. Global market conditions were impacted by events like the Russian invasion of Ukraine (2022), COVID-19 (2020), the housing market crash (2008), the 9/11 terrorist attack (2001) and an internet bubble (2000). In crisis times, the value of informed decision making is more critical than ever. The impulse to make hasty decisions in the face of crisis must be tempered with thoughtful considerations of reprioritization, divestment and even strategic investment.

Every decision that must be made carries some degree of risk, and explicit consideration of that risk will lead to better decisions. Even when decisions must be made quickly, a pragmatic assessment of organizational dependencies (risks) like technology, business continuity, workforce and third parties can create valuable insight to support success in all phases of a crisis.

Crisis events will significantly reshape an organization's risk profile and risk posture and put a spotlight on how organizations manage the uncertainty they're forced to deal with to survive. Risk management in a crisis is about a combination of minimizing the impact now, recovering as the crisis event resolves, and restoring and rebuilding when the crisis is over (see Figure 1).

Figure 1. Phases of a Crisis and Related Activity



Source: Gartner
727925_C

Gartner

A crisis creates immediate material pressure on organizations to control costs and cut where possible. Organizations must ensure that a singular focus on cost cutting does not create unacceptable risks in other areas of strategic importance. Organizational leadership will be forced to choose winners (preserve or invest) and losers (cut or divest) across every aspect of organizational operations, process, assets (including members of the workforce) and even goals. In doing this, they should take care to make wise informed decisions that do not needlessly mortgage the future.

In a crisis, organizations must assess four of the most material dependencies for current risk and future risk:

- **Technical debt** — Most organizational outcomes are largely dependent on technology. The readiness of that technology to support those outcomes should be managed. Technical debt can manifest in a variety of ways through poor decision making and neglect.

- **Business continuity** — Market crashes and crises typically result in failures of everything from technology to supply chains. Whatever its dependencies may be, the organization should consider the risk of decisions that impact running the business from response through to the recovery phases of a crisis.
- **Workforce readiness** — In a market crash, business and mission priorities change. New priorities need a new balance of skills, and old priorities may require divestiture. Organizations must consider opportunities in the recovery to create priorities for investing in developing new skills during the downturn.
- **Third-party risk management** — In addition to having the right partners to navigate a downturn, organizations will desire to divest suppliers that are less critical. These choices can save money, but also create risk if they do not have the right partners and suppliers to accelerate in the recovery.

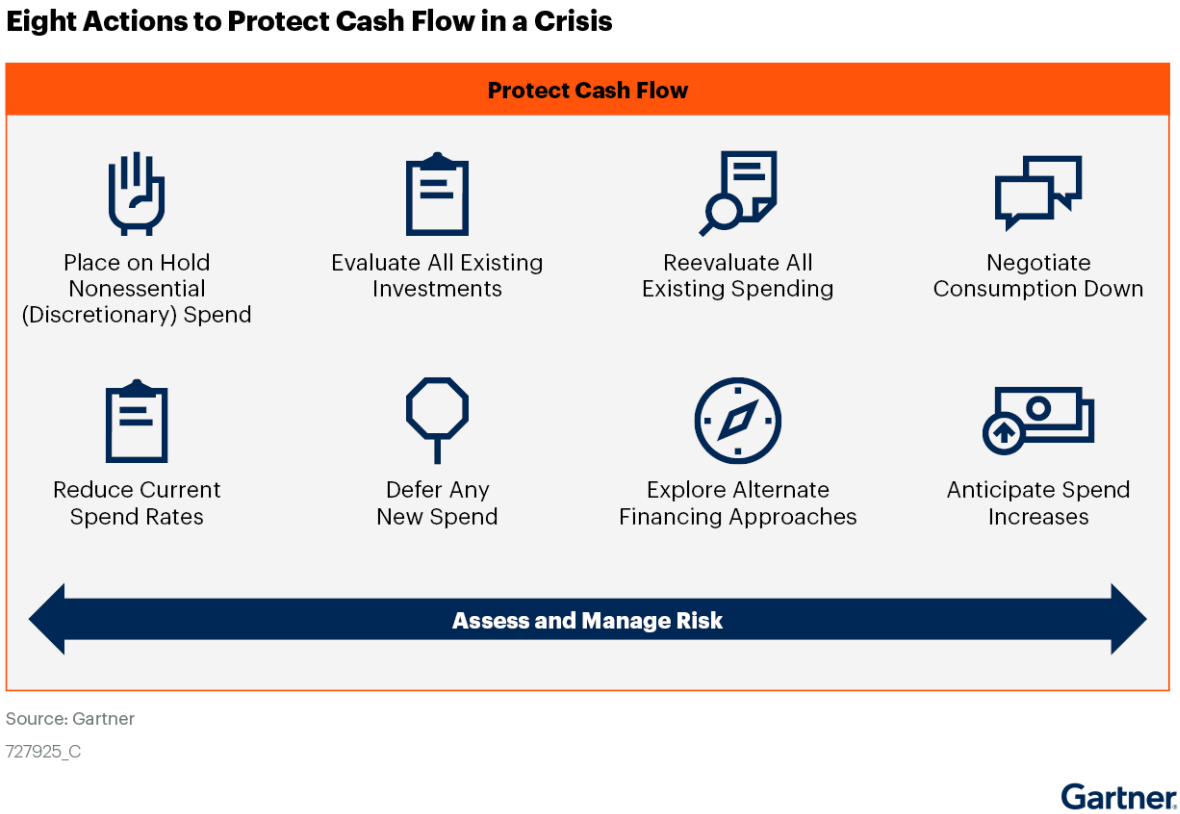
Analysis

Optimize Costs and Protect Cash Flow in a Global Crisis

Global crises like the Russian invasion of Ukraine and COVID-19 can lead to financial business implications in all industries and geographies. As economic impact grows, financial pressures increase, and enterprises that fail to act may not survive the disruption or will have their subsequent recovery delayed. Survival depends on careful management of commercial risk considerations in decision making (see 8 Actions CIOs Must Take During the Russian invasion of Ukraine for Financial Survival).

A fundamental contributor to enterprise survival in these situations is ensuring the organization's ongoing cash flow. With that in mind, executive leaders must assess, communicate and manage the subsequent risks when taking the actions in Figure 2 to protect cash flow.

Figure 2. Eight Actions to Protect Cash Flow in a Crisis



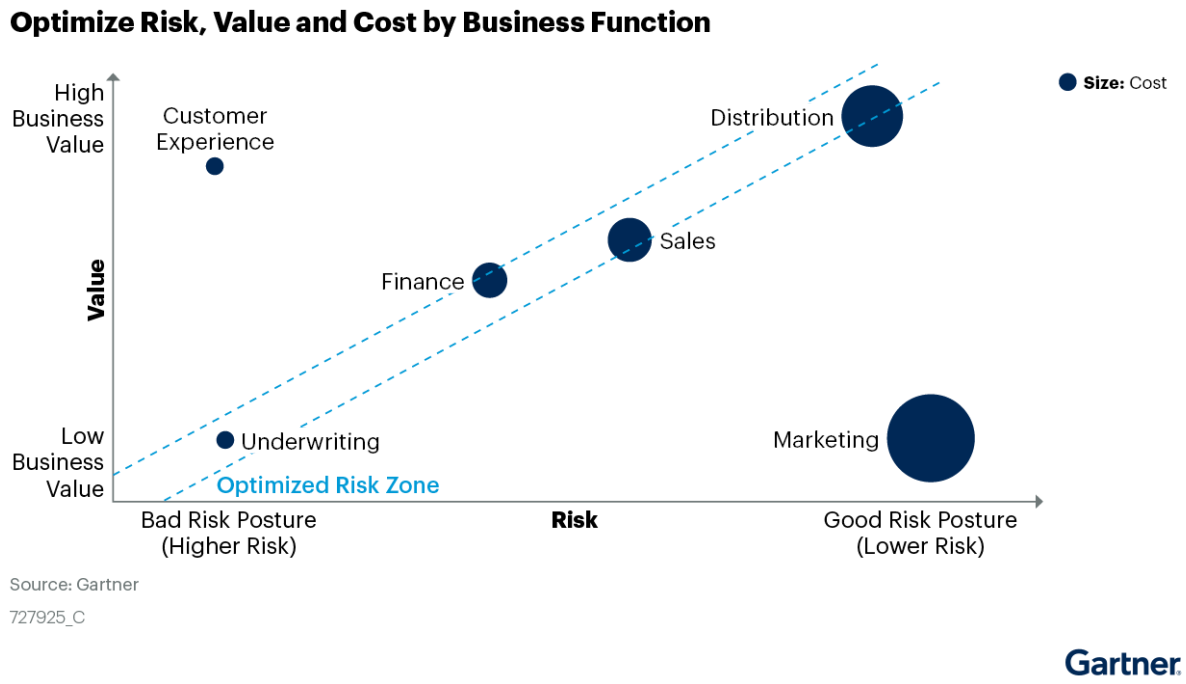
Executive leaders seeking to mitigate cash-flow challenges through IT cost and risk management should:

- Protect cash flow by assessing risk, cost and value in decision making. Cash is king and must be protected at all costs.
- Define new spend levels by identifying what the enterprise needs and how much it can afford to pay for that in a new harsh economic reality.
- Reduce strain on current cash flow by proactively canceling projects, eliminating services and reducing service levels. In addition, release unnecessary personnel, and renegotiate all business demand.
- Anticipate spend increases in essential areas for business continuity, while removing or at least freezing all nonessential spending.

When an organization must make immediate and aggressive decisions like these, it should understand, measure and consider risk posture in crisis-driven decisions. Business outcomes and priorities may have shifted and changed — as well as the levels or types of risks that executives are willing to take to achieve business outcomes. As the risk posture changes, the executive leader must effectively communicate the impacts of technical debt, business continuity, workforce readiness and third-party risk management (see Achieve Business Goals With Gartner's Risk, Value and Cost Optimization Decision Model).

The executive leader should plot the business value of business units, functions or outcomes against their readiness to address known risks and should include consideration of cost. This provides the executive leader a comparative analysis that supports priority and investment decisions (see Figure 3).

Figure 3. Optimize Risk, Value and Cost by Business Function



The bubbles in Figure 3 are business functions, but could represent business units, business outcomes, processes or product lines — that is, any unit that is understood to drive value within the organization. Each business unit has dependencies on technical debt, business continuity, workforce readiness and third-party risk management that are subject to changes in cost pressures and other crisis-driven decisions. It is through the double lens of business value for desired outcomes and risk created by these dependencies, that an organization can better guide decision making.

In this example, marketing has a well-funded technology stack that enables its business outcomes and effectively manages the risks of technology dependency. This is a positive outcome for marketing, when compared with other functions driving greater value for the enterprise (like customer experience) that have less funds invested in them and greater risk of failure. Thus, executives can begin to assess whether funding and focus are allocated correctly for the enterprise's broader risk management and value delivery.

Assess Technical Debt

Technical debt describes future liabilities that are created as the result of poor decision making. It manifests as technology problems impacting supported business outcomes across a variety of capabilities such as availability, usability, response time, throughput, scalability, reliability, performance, efficiency, maintainability, portability, security and compatibility.

The gradual accumulation of technical debt can lead to suboptimal performance in a portfolio, such that there will be significant and measurable negative impact on business performance. In a crisis, poorly considered decisions can lead to technical debt damaging business outcomes, ranging in severity from trivial to catastrophic.

Cybersecurity is a special class of technology debt that should be tracked separately, as it is both a board-level issue and a regulatory focus in many industries. Adding security controls to critical technology services is very costly after they have been established.

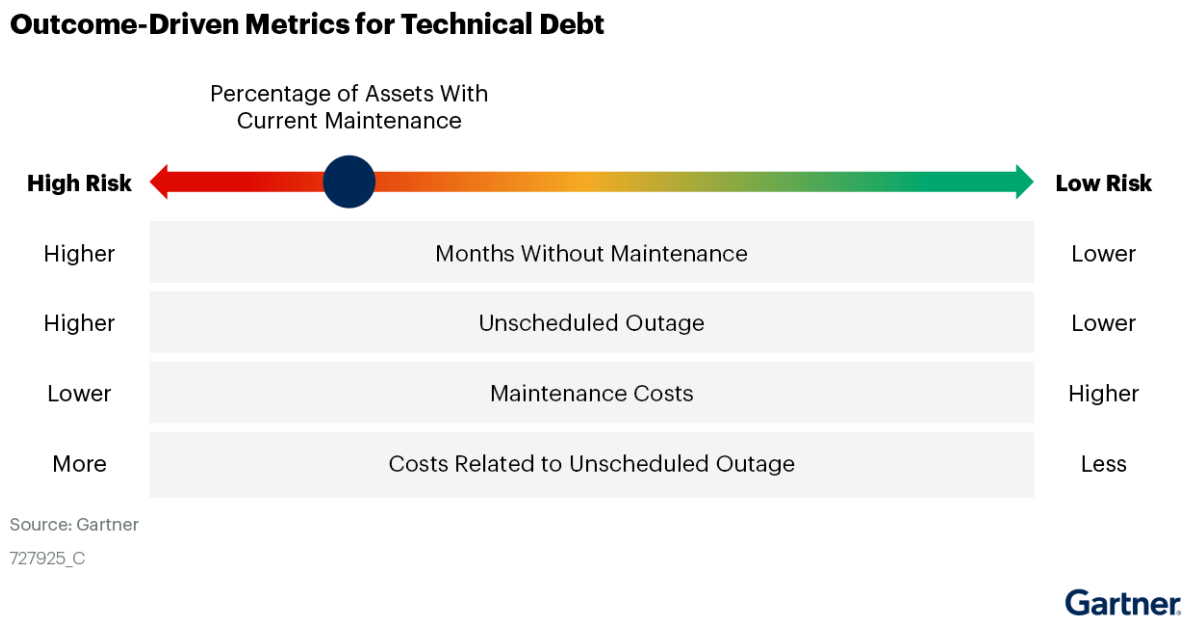
For example, one of the key technology dependencies that emerged very quickly during the COVID-19 pandemic was the need to support immediate remote workforce capabilities (see How to Cultivate Effective 'Remote Work' Programs). These crisis-driven decisions carry a lot of potential technical debt depending on how they are made. Seventy-four percent of companies surveyed during the pandemic said that 5% or greater of their workforce would remain working from home after the crisis was over. [1]

A consideration of technology debt in these crisis-driven decisions would point to investments in security, workforce communication and productivity technology to meet the demands of their new workforce reality. For example, if the companies ramp up operations and build business processes around technology that is not secure, they will face significant costs and risk in the future due to poor decision making during the crisis.

Figure 3 should be considered in the context of optimizing the risk of technical debt in the technology stacks supporting a variety of business functions. Technical debt is a measure of how well or how poorly the supporting technology stacks are maintained. This is also a reflection of risk to the supported business functions. Here, the level of technical debt experienced by each technology stack is plotted against the business value of the supported business functions and their business outcomes. This can be treated as a baseline for technical debt risk for decision making in a crisis.

One way to measure technical debt is with outcome-driven metrics (ODMs — see Outcome-Driven Metrics for the Digital Era). For example, an ODM measuring maintenance coverage and collateral cost and effects can be used to influence decisions to optimize cost by cutting maintenance. This ODM is measured by business unit to reflect the impact on business outcomes (see Figure 4).

Figure 4. Outcome-Driven Metrics for Technical Debt



Choices to accept technical debt without considering the impacts on business outcomes or cost can result in unacceptable risk that is not visible to executive decision makers. The CFO may cheer the lower costs but would lack full visibility into the risk of eventually facing a major investment to upgrade a failing infrastructure. So, this choice would not be credible or defensible to shareholders or regulators. In Figure 4, however, the organization chooses to measure technical debt that can represent risk posture on the x-axis. Thus, the organization plots the technical debt of each technology stack supporting the business outcomes, resulting in risk consideration during crisis-driven decision making.

Assess Business Continuity

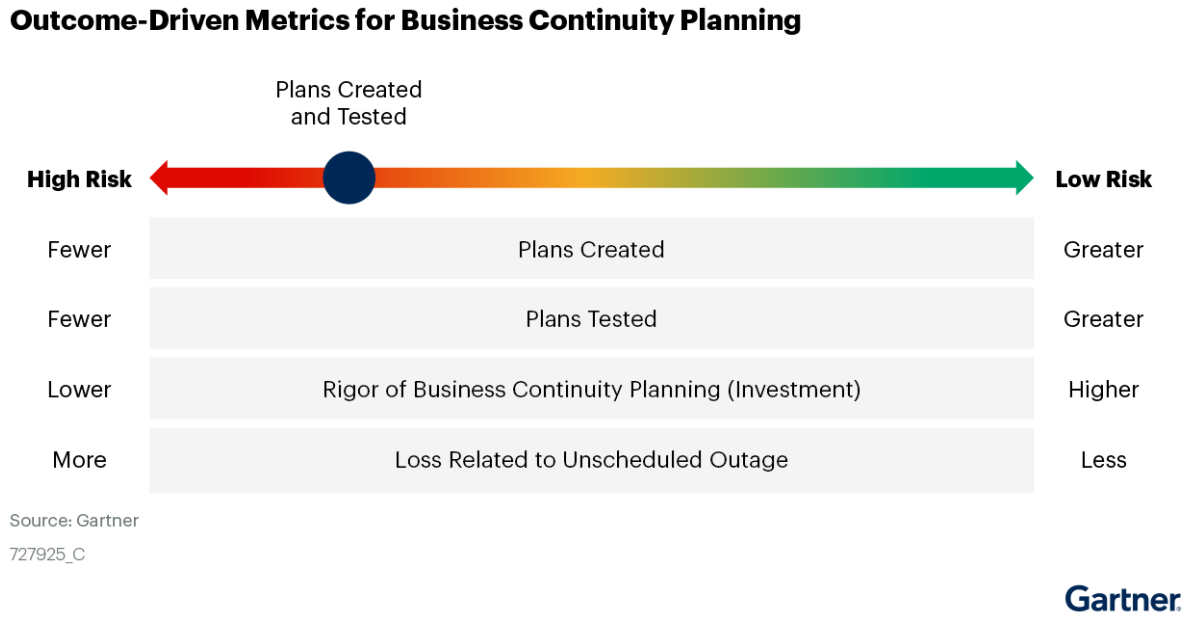
Business continuity management is concerned with the organization's continuous operations and delivery of products and services in the face of disruption. Business continuity management (BCM) covers the gamut of business recovery and continuity, IT disaster recovery and service continuity, supply chain risk management, and crisis management and communications.

Good BCM is more about good planning and preparedness than about execution at the time of disruption. Organizations that have mature BCM programs are more likely to minimize the impact of crisis-led disruptions to their operations and revenue sources, while quickly pivoting to their alternate strategies for business continuity.

During a crisis, organizations should use the knowledge, assessments and analysis of business operations embedded in business continuity plans to inform crisis-driven decision making.

Measuring and understanding the state of business continuity across the organization and its business processes and outcomes can provide critical context in crisis decision making. This can be tracked, for example, through ODMs measuring the state of business continuity plans created and plans tested for each business process (see Figure 5).

Figure 5. Outcome-Driven Metrics for Business Continuity Planning



When we go back to Figure 3 again, this time, the business continuity ODM can represent risk posture on the x-axis to plot the business continuity readiness of each business process supporting the business outcomes. This visibility into the business continuity readiness of business units and product lines can be used to influence or accelerate crisis-driven decisions. It can also be used to mitigate risks previously deemed acceptable or avoid creating risks to resuming normal business operations throughout the response and recovery phases of the crisis.

Workforce Readiness

Workforce changes are a likely outcome in any crisis that includes a material change in operational or economic conditions directly impacting the organization. In crises that impact revenue and operations, like the Russian invasion of Ukraine, some organizations will need to relocate and support employees in areas directly affected by conflict. They must also address workforce size and makeup throughout the rest of the organization to address economic realities, market changes and labor needs (see Sustaining Workforce Resilience Through Disruption).

Consideration of risk in these decisions can balance actual potential savings against risks like operational continuity and the challenges of restaffing during the recovery and renew phases. Decisions will need to address some workforce segments that were forced to change and protect other segments. The two most common failures are applying a blanket measure to all departments and targeting the highest spend workforce. Both can be problematic in terms of potentially removing capabilities needed for the future.

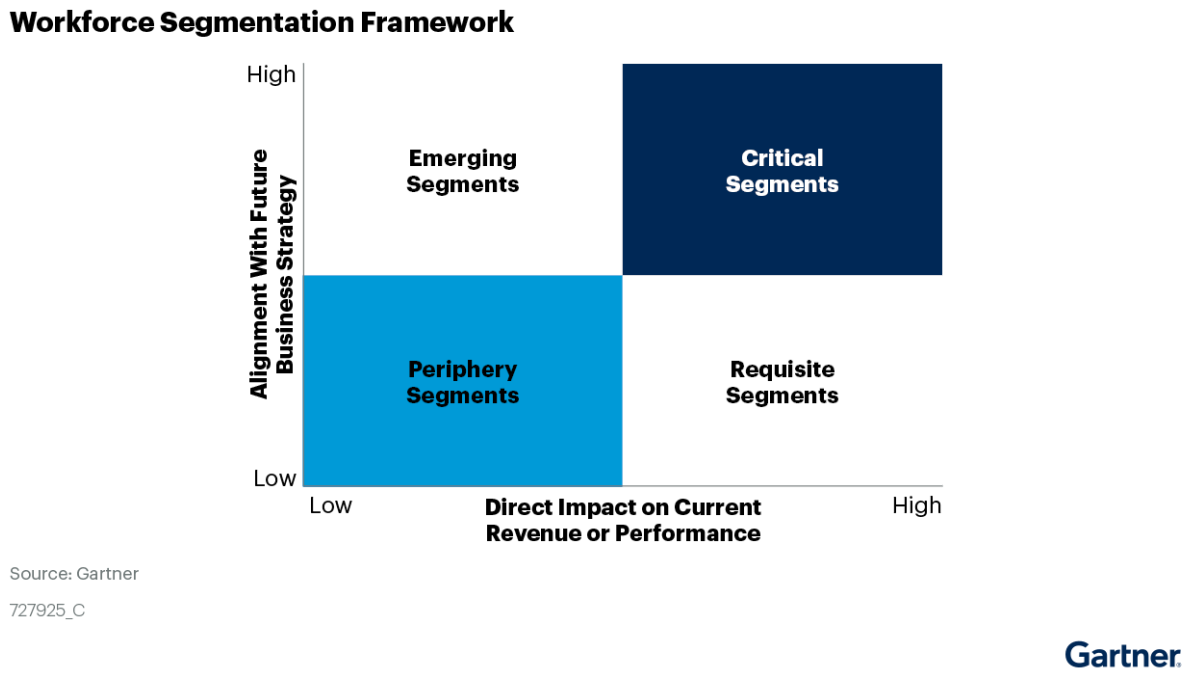
Business stakeholders crafting proposals for workforce changes, especially in times of crisis, may become fixated on only short-term implications to the bottom line — namely, cost. The IT HR leader is uniquely positioned not only to help the senior leadership team assess cost, but also to focus on protecting the most valuable contributions that the workforce makes to the organization. These efforts to identify target segments must ultimately address two questions:

- How much risk would changing that workforce segment create to the future business strategy?
- How much value does that workforce segment generate for the current business?

Plotting each workforce segment on the framework in Figure 6 by its relative alignment with future business strategy (y-axis) and level of impact to current business performance (x-axis) can help answer and balance those two questions. Doing so categorizes workforce segments into the four quadrants of this framework: periphery, emerging, requisite and critical.

Such a model provides a simple landscape to help leaders judge the workforce segments' relative level of impact on the enterprise's ability to survive the downturn, quickly recover or grow in a postcrisis environment (see How to Make Workforce Reduction Decisions Using Segmentation Strategies).

Figure 6. Workforce Segmentation Framework



The framework can help guide leaders to successfully manage selections that best enable survival and innovation during the economic downturn, and recovery and growth after it. It helps avert reactionary responses to worsening economic conditions that lead to short-sighted layoffs with unintended consequences for current performance and future business growth.

Assess Vendor and Third-Party Risk Management

Organizations typically have multiple partners on which they depend to deliver their organizational outcomes. In a crisis, an organization will be forced to make decisions over which partners to keep, which to drop, which to pay, and which to negotiate severance or new terms.

Many larger organizations will have formal third-party risk management plans. These should include a criticality assessment with risk tiering based on the criticality of a business process managed or supported by a vendor. If the organization does not have one of these assessments as it enters a crisis, there is material value in creating one at any level to guide decisions. The risk tiers should be as follows:

- **Mission-critical** — The supplier supports or performs a vital core function that is critical to the organization's survival. If this function were unavailable, then there would be a threat to the organization's ability to stay in operation, leading to irreparable damage.
- **Critical** — The supplier supports a critical function that is important to maintain the operations of the organization. If this function were unavailable, then it would lead to a regulatory breach, financial or reputational loss, or widespread negative press coverage leading to loss of clients or market share.
- **Important** — The supplier supports a function that is involved in the ongoing operation of the organization.
- **Deferrable** — The supplier supports a function that is noncritical to the organization.

An assessment of impact should also be performed relative to the business goals. An impact scale provides a hierarchical set of levels to estimate the anticipated level of loss, damage or other form of impact that would result if there was a failure to meet one of the business objectives (see Formalize Vendor Risk Management Practices to Lessen the Probability of Business Disruption).

The assessment results (vendor risk score) can be used as an ODM to reflect business outcomes at risk from their dependency on vendors at risk (see Figure 7).

Figure 7. Outcome-Driven Metrics for Third-Party Risk Management

Organizations can also benefit from a consideration of risk, value and cost in the context of third-party support for business outcomes. Using Figure 3 again, the business outcomes and business values remain the same. Cost (bubble size) is based on the costs and investments in the vendors that support each outcome.

The vendor risk ODM can represent risk posture on the x-axis to plot the readiness of the vendors supporting each business process and related business outcome. In a crisis, it is valuable to have the context of vendor dependencies where there is already risk. Does the crisis exacerbate any identified risks and raise the priority of divesting from certain vendors? Do dependencies exist that create unreasonable risk to business outcomes by divesting from certain vendors?

Track Risk in All Phases of a Crisis

As organizations move from response to recovery, they will have to start paying the bills for poor decision making earlier in the crisis. Canceling maintenance creates technology debt. Moving people from offices to working from home creates security requirements. Laying off people with critical skills impacts recovering operations. Divestment of partners and vendors limits scalability.

Some of those bills will be due sooner, and some will come later. The best way to manage these costs is to record risks that are understood and accepted, as decisions are made, so appropriate planning can guide the enterprise's investment through the recovery and renewal phases.

Evidence

[1] Global Economic Effects of COVID-19, Congressional Research Service (downloads PDF)

Document Revision History

Manage Risk in Crisis-Driven Decisions From Response Through to Recovery - 8 June 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription. A

Decision Model to Optimize Risk, Value and Cost

Optimize Risk, Value and Cost in Cybersecurity and Technology Risk

The Urgency to Treat Cybersecurity as a Business Decision

Outcome-Driven Metrics for Cybersecurity in the Digital Era

The CARE Standard for Cybersecurity

An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making

Managing Enterprise Outcome Risk: Risky Decisions Are Risky Business

Use Our Decision Model to Optimize Risk, Value and Cost in Governing Portfolios

8 Actions CIOs Can Take During the Russia-Ukraine War for Financial Survival

---

Connect With Us

Get actionable, objective insight to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Stay connected to the latest insights

Attend a Gartner webinar

View Webinars

Gartner®