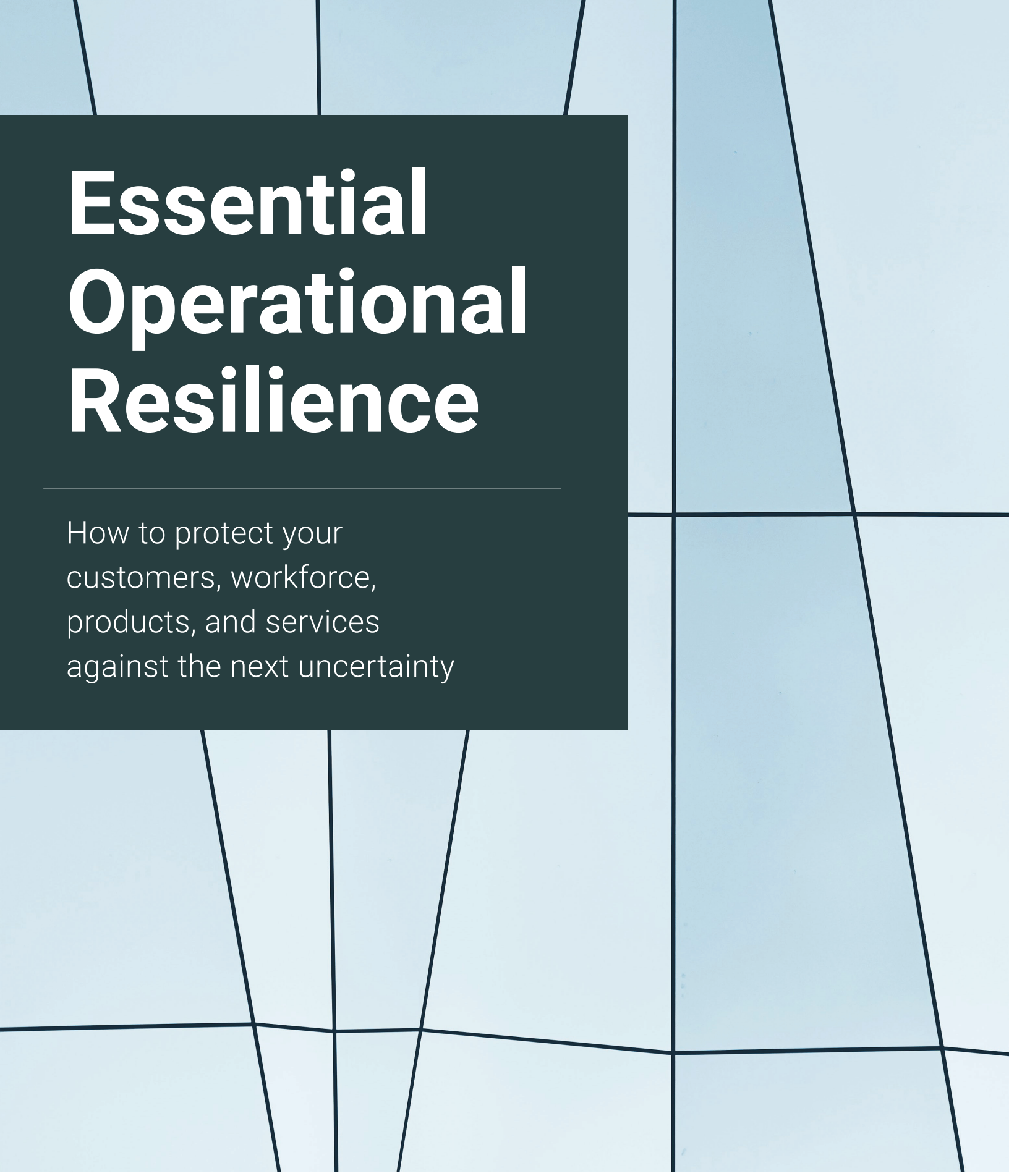


Essential Operational Resilience

How to protect your customers, workforce, products, and services against the next uncertainty

OCEG®
Driving Principled Performance

SPONSORED BY servicenow

ABOUT

OCEG is a global, nonprofit think tank and community of more than 85,000 members, dedicated to helping organizations reliably achieve their objectives, while managing uncertainty and acting with integrity.

This is what OCEG calls Principled Performance, and it is a goal that every organization can achieve by integrating and aligning their approaches to the governance, assurance and management of performance, risk and compliance. Processes for achieving that integrated approach, commonly called GRC, is supported by the open source standards set out in OCEG's Red Book GRC Capability Model. OCEG™, LeanGRC®, Principled Performance™ and Driving Principled Performance™ are trademarks of OCEG.

Learn more at oceg.org

ServiceNow (NYSE: NOW) is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for employees and the enterprise.

ServiceNow Governance, Risk and Compliance helps power your resilient business with risk-informed decisions integrated across the enterprise so your people and organization work better. By seamlessly embedding risk management and compliance into your digital workflows and familiar user experiences, you can improve decision-making, increase performance, and gain real-time visibility into risk. Only ServiceNow can connect the business, security, and IT with an integrated risk framework that transforms manual, siloed, and unfamiliar processes into a user-friendly, unified program built on a single platform.

Learn more at servicenow.com/risk

AUTHOR

Barbara G. Kay, GRCP, CISSP, leads product marketing for security and risk at ServiceNow. She has been laser focused on security and risk management for more than 15 years. Barbara co-authored "Digital Transformation and Risk for Dummies".

INSIDE THIS BOOK

OPERATIONAL RESILIENCE: the ability of an organization to continue to serve its customers, deliver products and services, and protect its workforce in the face of adverse operational events by anticipating, preventing, recovering from, and adapting to such events. This is an essential element of Principled Performance -- the ability to reliably achieve objectives while addressing uncertainty and acting with integrity.

INTRODUCTION

"Pivoting isn't throwing a dart on the map and then going there. It's changing direction or changing your path to get somewhere based on what you've learned along the way. Once you've pivoted and are on a new track, that becomes your new Plan A."

Reid Hoffman, "The Startup of You"

Although LinkedIn Cofounder and Executive Chairman Reid Hoffman's guidance on the value of having a Plan B was designed for individuals navigating their careers, it's proven on-target for business leaders steering organizations through staggering operational challenges sparked by a global pandemic.

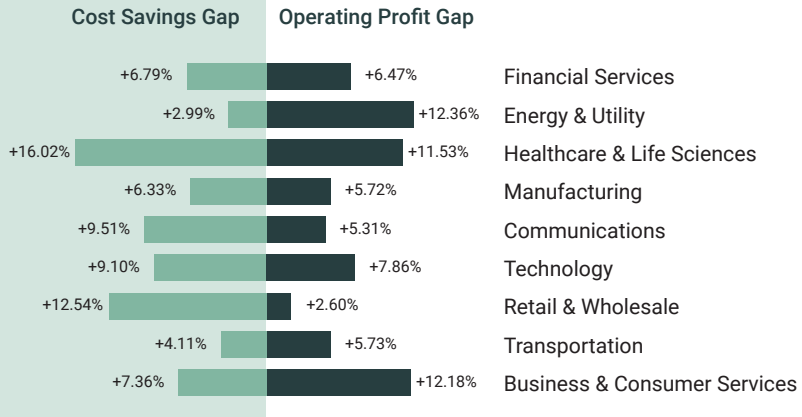
COVID-19's far-reaching impacts have thrashed many companies' Plan-A strategies, yet the pandemic offers rich learning opportunities on operational resilience. Leaders will need these insights to navigate crises and disruptions that will arise long after this coronavirus subsides. Just ask executives within any of the many organizations whose operational resilience enabled them to quickly respond, recover and adapt to the supply chain havoc, business closures, sweeping shift to remote work, liquidity risks and other COVID disruptions.

After contending with supply shortages during the SARS outbreak, 3M adapted its processes, including localizing some of its supply chains, so it could swiftly ramp up production to address sudden spikes in demand for respirator and related personal protective equipment (PPE). In the financial services realm, Hong Kong-based insurer Ping An leveraged the global financial crisis to establish a more diversified subsidiary, Ping An Technologies, whose focus on cloud and other advanced technologies has helped its parent company sustain its torrid growth throughout the past decades. What these and many other companies have in common, according to Boston Consulting Group (BCG) research[1], is that their operational resilience has enabled them to out-perform other companies by 30 percent, based on the measure of total shareholder return, during periods of crisis.

While operational resilience is rightly promoted as a protective capability, ServiceNow research shows that digitally advanced companies with strong operational resiliency capabilities also gain tangible value. It will be important to keep these dual benefits in mind as savvy leadership teams leverage the current crisis for lessons to systematically strengthen resilience, via a well-defined plan and structure, before future crises arrive, as they assuredly will.

The digital leadership advantage, across industries

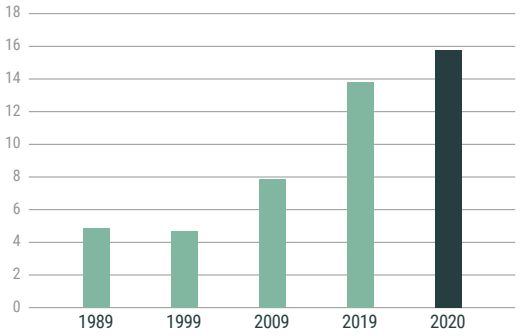
Leaders spend less and book greater profits than digital laggards



ServiceNow research in 2020 indicates that digitally transformed companies do better on cost management and operating profit, with performance varying somewhat by industry.

Source: workflow.servicenow.com/c-suite-library/digital-leaders-outperform-in-covid-19-era/

Although operating realities changed dramatically during the COVID pandemic, significant business disruptions have been growing more common for decades. With our global economy and interdependent business operations, we are now more at the mercy of external forces such as extreme weather events, trade wars, geopolitical conflicts and cyberattacks. The average cost of a data breach to U.S.-based companies reached 8.64 million in 2019, according to Ponemon Institute.[2] Through September, the year 2020 had already yielded 16 $1Billion disasters in the US alone.[3] This isn't an outlier: the number of $1B disasters annually in the US has tripled since 1999.



The number of $1B natural disasters in the US has tripled in the last 20 years.

ncdc.noaa.gov/billions/events/US/1989

Disruptions have a ripple effect. Consider a company that provides payroll processing services to businesses. If that service goes down for 24 hours, the customers' customers —parents, students, families—will not get their paycheck in time. If the payroll provider uses its own services, the outage also will result in a lot of unhappy employees. Each risk management decision is amplified when the impacts of those decisions also affect the workforce and customers.

While most adverse events have a short time span, COVID has demonstrated the steep human, economic, and health and safety impacts of a long-term disruption.

Global corporate directors and C-suite executives rated the "impact of regulatory change and scrutiny on operational resilience, products and services" as their topmost concern this year, according to "Top Risks for 2020" research conducted by Protiviti and NC State University's ERM Initiative.

The situation is more urgent and challenging than in years past. Complex businesses, distributed locations, and multiple third parties create brittle systems. One break can unravel the whole thread, whether you build cars, financial services, or pharmaceuticals.

Risk and resilience are now at the top of board and C-suite priority lists. Global corporate directors and C-suite executives rated the "impact of regulatory change and scrutiny on operational resilience, products and services" as their topmost concern this year, according to "Top Risks for 2020" research conducted by Protiviti and NC State University's ERM Initiative. While operational resilience also figured as a major concern among directors and executives within the financial services industry, that segment of survey respondents was even more concerned about the disruptive impacts of competition from "born digital" competitors -- a threat that stout operational resilience can mitigate.[4] Clearly, business leaders have the responsibility to prioritize investment in operational resilience across their organizations and within their spans of control. This preserves their organization's ability to deliver services, protect their workforce, and meet customer expectations—even if they can only do so with degraded services.

This paper will help business and risk leaders understand the issues and set direction based on an actionable lifecycle. Each organization's industry, risk posture, and economic outlook will color their approach within this framework.

[1] bcg.com/en-us/publications/2020/how-to-become-an-all-weather-resilient-company
[2] ibm.com/sg-en/security/data-breach
[3] ncdc.noaa.gov/billions/events/US/1989
[4] protiviti.com/sites/default/files/nc-state-protiviti-survey-top-risks-2020-executive-summary.pdf

PRACTICAL OPERATIONAL RESILIENCE

What is resilience at a practical level? Resilience demands you understand your organization's critical success factors and points of failure. It means you can execute plans to ensure that the things you and your customers care about can keep going and remain safe under duress. Your success at resilience will vary greatly depending on your proactive planning and ongoing execution. The more distributed and dynamic a business is, the more frequently its risk factors should be monitored and managed; leading companies do so in real time.

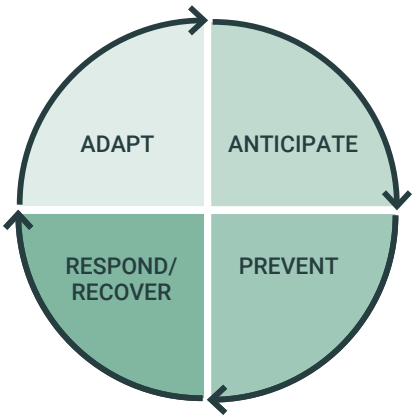
The COVID pandemic has taught us we have to expand our thinking, both strategically and inside the organization. We must go beyond functional silos to consider the overall organization and its operational interdependencies. For example, what can go wrong with the supply chain? What people does it depend on? What happens to customers if it breaks down? The more you explore these issues up front, the more likely you are to navigate effectively through a real situation.

- Manufacturers need a productive workforce, safe facilities, and an intact supply chain so they can design, build, and deliver products.
- Retailers need reliable manufacturers and suppliers to stock their virtual and physical shelves.
- Digital service vendors depend on their marketing engines, support teams, billing systems, and technology infrastructure. These may all have IT, workforce, content, and cloud provider partners.
- Financial services providers need to ensure that their critical third party providers—of cloud technology services, analytical insights, and more—operate in a resilient manner while maintaining compliance with all relevant data security and privacy regulations.

It is important to keep in mind that resilience requires participation across the typically siloed people, processes, and technology that operate your business and manage risk domains. The goal of integrated risk management tools is to help you organize teams and monitoring around the four pillars of people, technology, facilities, and suppliers, as well as the layer of processes they support, while helping you roll up information to support functional groups and stakeholders.

You'll need leaders to make specific people responsible and accountable for these pillars, as well as oversee the overall program.

One success factor for resilience is getting access to accurate data from wherever it lives. Effective assessments, planning, and—especially—actions often hinge on sensitive data from your finance, HR, IT, vendor, and facilities systems. Ensure your resilience plan includes a complete and secure model for automated data sharing across data sources like these. Ideally, this data uses a shared data model to ensure data accessibility, accuracy, and security. The fewer ad hoc phone calls, spreadsheets, and emails involved in your program, the better will be your accuracy, efficiency, and accountability.



A FOUR-STAGE LIFECYCLE

We recommend establishing operational resilience by building a continuous four-stage cycle: anticipate, prevent, respond / recover, and adapt. These activities do not necessarily follow a fixed sequence. Practitioners often iterate between anticipate and prevent, as they learn through testing that business needs change and priorities must be reset in response. Iterations are also natural as you respond and adapt within the process of recovery. As we are seeing with COVID, there are adjustments, detours, and inventions required to get through and beyond an adverse event.

Stage 1: Anticipate

By investing time up front, you focus resources and get better results through the rest of the lifecycle. The process starts by taking a step back and thinking strategically about two things: what you need to care about based on what's essential to serving your organization's customers, workforce, and products and services, and what could go wrong.

As you inventory, think about the different things your business depends on:
People: Employees, consultants, staff from third-party service providers, and customers
Processes: Communications and collaboration systems, information systems, regulatory and governance oversight
Technology: data, applications, infrastructure, access to systems and services
Facilities: physical locations (offices, stores, warehouses, manufacturing facilities, data centers), as well as the capabilities required for these sites to fulfill their function, including providing environmental, health, and safety of the people who use them
Suppliers: IT vendors, parts suppliers, service providers, outsourcing partners, and consultants

To tackle this holistic list, prioritize based on impact. Rather than a massive spreadsheet, the modern tool for managing this process is a Business Impact Analysis, typically part of a business continuity management or integrated risk management suite.

Take a deep breath. This isn't once and done. You'll need to establish the rigor to revisit periodically based on the criticality of the systems (more frequently for more important systems), changing risks to your business, if your systems and processes change significantly, or when there's a significant change in operating conditions. The more important it is, the more frequently you should revisit the plan. At a minimum, we recommend an annual review of the business impact analysis prioritization. That review should include cross-functional team members for a realistic assessment.

Here is the "anticipate" process:

1. Inventory customers, products, services, key personnel, processes, vendors, facilities —identify the key factors in fulfilling your organization's mission.
2. Identify dependencies among them. Document the critical relationships and points of failure that could lead to a disruption in the business.
3. Prioritize based on value to the business. Evaluate the impact of disruption to the company, using this information for prioritization.
4. Assess types and likelihood of risk to them.

For the risks you can't tolerate, your options are to treat, transfer, or terminate.

Stage 2: Prevent

The "anticipate" process has identified the important products and services, critical systems, the key risks, and the list of dependencies. Now, you are looking for ways to manage the risks. For the risks you can't tolerate, your options are to treat, transfer, or terminate. Treating involves proactive controls, automated monitoring systems, and detailed plans and training. Risk transfer is typically accomplished through insurance. Tolerate means you choose to accept it—although we've learned in 2020 that some things we thought we could accept have turned out to be extremely painful if not fatal. Terminate means you change or end use of a process. This might be the case for a third-party data center on a flood plain.

This prevent stage focuses on the risks you choose to treat. It includes the enabling processes and systems to minimize the likelihood and impact of adverse events.

Get comfortable. This phase takes the most time initially, and you will live here until you need to respond (the next phase) or revisit the anticipate phase.

The risk management infrastructure required for this phase will look very different from old-school, batch-oriented compliance systems. Business continuity management systems provide support for planning your approach and testing your systems in different scenarios.

Typically, existing controls will be tuned and extended, applying risk management policies.

Cybersecurity preventative controls and investigative procedures can be increased to offset specific risks like phishing, targeted attacks, and data breaches (big concerns resulting from the disrupted working conditions of COVID.)

- Critical IT systems can be architected with redundancy and employ a robust disaster recovery plan. You may choose to add on tools that can predict future service concerns based on past or likely behavior. Many companies see this as reason to adopt cloud and hosted services that may be more flexible and resilient than on-premises systems housed in a physical data center at risk of hurricanes and flooding.
- Contracts with materially important vendors, suppliers, and consultants should be reviewed and updated to meet recovery time objectives. You may also require specific risk assessments, mitigations, and reporting.
- Customer service systems may be restructured to provide better support for call deflection and digital self-service, as an offset to employees or contract services becoming unavailable.
- Employee support systems can be enhanced with tools for secure, multi-channel communication to and from the employee.
- Legal, public relations, and regulatory compliance teams should be part of crisis and emergency management planning and execution, to encompass potential risks to safety, reputation, and regulatory obligations.
- Cross-functional response teams can be designed, trained, and equipped with modern tools for success under pressure: automated, multi-channel notifications, on-demand crisis bridges, and mobile apps to help individuals track events and take or approve steps in plans.

The systems you build as controls must integrate with your monitoring to remove uncertainty, delay, mistakes, and effort. Not only does this make you more effective and efficient in terms of clock time, but most organizations also discover that automating paper, spreadsheet, and ad hoc processes save operational costs.

Appropriate and timely monitoring reflects external and internal events. Ideally, critical data sources should stream feeds or alerts that your tools can normalize, correlate, filter, organize, and factor in to risk calculations and thresholds. With or without a human in the loop, this situational intelligence is essential to initiate action. In addition to news and government sources, factor in external inputs from the systems you depend on but may not control: cloud, XaaS, and third-party systems.

In terms of the things you can control, embed automated tracking via indicators within your internal IT, security, HR, customer, and environmental systems. You should also build in ways to make it easy for people to report and update changing risks. This is the era of "mobile-first," and that communication path is even more important in a crisis.

Once you have your people, process, and technology in place, and you've tested them against the scenarios you defined up front, you will mostly be monitoring to respond as quickly and appropriately as possible to contain any impact. Of course, there will be updates and tuning as your systems and your business evolve.

Integration of this program with your overall operational risk management program will reduce the burden on your second line and simplify alignment across functions. It also improves the speed and accuracy of reporting to all your stakeholders. Since you are protecting the entire business, this may include a broad range of people inside and outside the company.

The "prevent" steps include:

1. Establish controls that may include processes, alternate vendors, monitoring, incident response programs, health & safety monitoring, communication systems and plans, disaster recovery plans, and reporting dashboards and distribution mechanisms.
2. Test controls and plans against predicted scenarios, such as fire, hacking, pandemic, and geopolitical unrest
3. Adjust controls based on findings during the test
4. Monitor risk indicators to detect changes you should account for
5. Monitor for adverse events that might trigger activation of a plan
6. Communicate status to stakeholders at the frequency and detail defined in your plans
7. Revisit plans and controls as systems and risks change (see "anticipate")

Stage 3: Respond and Recover

When each inevitable adverse event happens, your goal is to execute plans with confidence to minimize the impact on your customers, workforce, and products and services.

Expect the unexpected. An initial crisis response may resolve quickly or require a protracted recovery. There may be unpredicted consequences and side effects, particularly since your community and public infrastructure may not be as prepared as you are.

Depending on what you are dealing with, you may be running multiple parallel actions—crisis response, containment, and recovery—in different regions. You may need to learn and adapt while you are recovering. Response phase complexity creates a stressful environment that can be improved by the guardrails of policies, plans, and practice.

Response phase complexity creates a stressful environment that can be improved by the guardrails of policies, plans, and practice.

Monitoring (automated and human) should trigger your action plans for effective response, containment, and rapid and safe recovery. The business continuity and communication plans and programs you built in the 'prevent' phase go live now, initiating the processes and teamwork required.

The controls and monitoring you created beforehand provides essential visibility and detail to support response teams and keep your stakeholders aware and aligned. Systems collect data that helps you in the moment, as things unfold, and provide critical inputs for the adjustments and debriefs that will make you more resilient afterward.

"Response and recovery" steps include:

1. **Activate plans** for adverse event or emergency
2. **Execute** each plan
3. **Communicate** adverse event to all who are affected or must be informed
4. **Refine** systems and processes (including reassignment of staffing and deployment of additional support) as needed for changing conditions
5. **Restore** services, processes, and systems when it is safe to do so

Step 4: Adapt

In this final phase of the lifecycle, your goal is to glean as much as you can from the experiences you've had so you can refine your program to perform better the next time. There's a saying that "no plan survives first use." You've just activated multiple plans, so this phase has you assessing each of them to find the cracks and opportunities for improvement.

This phase balances formal and structured processes with sensitivity to the nature and potential trauma of the situation. Many different people will have been involved in response or affected by its success, so you must make it easy to identify affected systems, plans, or steps that didn't work well, and ideas for change. Collect qualitative insights in advance from people using anonymous surveys, and extract relevant quantitative data from your systems. Core team members should then engage in a debrief that reviews these two data sets and recommends changes.

You may learn things that affect every part of the resilience lifecycle—what systems turned out to be business-critical, the weak links in those systems, or the impact of key personnel not being available. It's likely your plans and monitoring had some blind spots that you can fix with new or improved controls and indicators. In some cases, regulations and governance policies will change, either temporarily or permanently. Stakeholders and executives may demand new metrics and reports.

Investing time in this stage will help avoid knowable problems in the future. People and the press are less forgiving if you don't deliver a better performance the second time adversity strikes.

The "adapt" phase includes:

1. **Identify root cause** for damage, problems, and errors
2. **Collect input** from participants on the effectiveness, accuracy, and learnings from the execution of plans and the actual response and recovery processes
3. **Engage** stakeholders and request support for required or recommended changes
4. **Address** ineffective controls (see prevent stage)
5. **Establish** new controls
6. **Update** plans and monitoring

ENGAGE LEADERSHIP

Now that you understand how to achieve operational resilience, the first step on your actual journey should be to enlist a cross-functional stakeholder team. Because of the scope of potential impact, you will want to have support from leaders who can approve and encourage participation, including breaking down some barriers that may be entrenched. They will also need to fund tooling and maintenance processes to keep the lifecycle alive.

On the upside, this initiative can help align organizational priorities and nurture the executive collaboration critical to long-term business success. With clarity on goals and roles, each leader can manage their teams to zero in on effective operational execution.

CONCLUSION

COVID's massive disruptions to products, services, suppliers, customer and employees have driven home the need to think more proactively, creatively and rigorously about what truly enables organizational mission and performance. The pandemic also has exposed the high, even existential, cost of ineffective operational resilience while demonstrating the high value—that 30 percent total shareholder return premium—of a systematic approach to building and maintaining robust resilience.

A structured framework for developing and sustaining operational resilience helps companies engage the right stakeholders while contributing to organizational success by:

- Helping leaders make thoughtful choices about what matters to the business and implementing systems and processes to proactively mitigate risk
- Replacing limited, siloed crisis communications and disaster recovery efforts with enterprise-wide, automation-enhanced action plans
- Reducing the disruptions that adverse events inflict on customers, suppliers, employees and other stakeholders
- Inspiring more confidence among all stakeholders in the organization's ability to thrive as the frequency, scope, and diversity of disruptions increase
- Driving effective and collaborative plans that span functional boundaries to protect revenue, productivity, and business continuity

While COVID-19 marks a historical turning point, the disruptions it has produced can and will be generated by other sources, including global trade skirmishes, intensifying cyberattacks, geopolitical unrest, natural disasters, and supply chain shocks caused by dozens of different factors.

"The world is becoming turbulent faster than organizations are becoming resilient," warns a Harvard Business Review article. "The evidence is all around us. Big companies are failing more frequently. Any company that can make sense of its environment, generate strategic options, and realign its resources faster than its rivals will enjoy a decisive advantage. This is the essence of resilience. And it will prove to be the ultimate competitive advantage in the age of turbulence—when companies are being challenged to change more profoundly, and more rapidly, than ever before."[5]

While those points crystallize the challenge that business leaders confront right now, the article, "The Quest for Resilience," was published 17 years ago. Operational resilience does not require a long and arduous search; it simply entails understanding, executing and sustaining a four-step framework. All the more reason to get started on Plan B today.

For more information, visit servicenow.com/risk.

[5] hbr.org/2003/09/the-quest-for-resilience

OCEG is a nonprofit think-tank with over 85,000 members that helps organizations drive Principled Performance® and enhance culture by providing standards, tools and resources to integrate governance, risk, internal control and compliance processes. OCEG®, LeanGRC®, Principled Performance® and Driving Principled Performance® are trademarks of OCEG.