The Ultimate Guide to Organizational Resilience

7 Building Blocks of Organizational Resilience

How to Support a Hybrid Workforce
as Attack Surfaces Expand

Content

Overview

Resilience remains a trending topic among organizations and individuals. The past 18 months have brought about an abundance of change. Organizations and individuals that can find meaningful ways to practice resilience in the face of change, from remote and hybrid working to digital acceleration, are at a significant advantage.

Remember, change for the sake of it is never a good idea. What we're discussing here is strategic and necessary to enable continued success. Think digital transformation, remote working technologies, etc. After all, being at the forefront of new technology and techniques can not only take companies forward but also give them a competitive advantage.

Resilient organizations are receptive to change rather than being rigid in their stance. They know the competition is fierce and it doesn't take much to be displaced. You can't count on last year's strategy to deliver effective results in tomorrow's ecosystem.

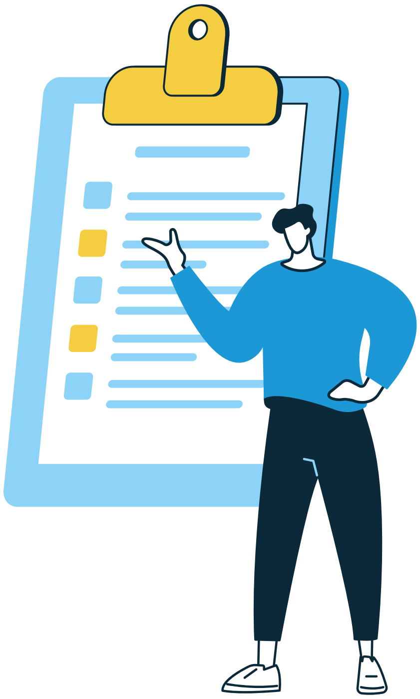
Resilient organizations and leaders are always looking ahead and asking questions like:

- Are we differentiating on value or price?
- What could displace us?
- How can we be more effective? How do we measure effectiveness?
- Are we measuring the right KPIs?
- What else do our customers need that we're not providing today?
- How can we help our employees better serve our customers?

These are the questions that keep leaders across organizations up at night, regardless of whether they are CEOs, CFOs, CTOs, CMOs or mid-level managers. Building a culture of resilience can help your organization resist the urge to sacrifice innovation for comfort.

In this "Ultimate Guide," you'll gain a working understanding of how to implement the 7 building blocks of organizational resilience into your framework:

1. Audit
2. Prioritize
3. Change
4. Accelerate
5. Sustain
6. Agility
7. Trust



Read on to discover what makes up the DNA of resilience and how to graft it into your existing decision-making processes to yield more sustainable outcomes. This involves adopting a mindset shift from short-term, quarterly-based thinking and metrics to a more holistic, long-term strategy for success that extends beyond a few good leaders and their tenure with your organization.

Adapting to a Rapidly Changing Environment

The COVID-19 pandemic pushed organizations across the globe into a whirlwind of change. Many organizations had to learn how to work completely remotely for the first time in order to meet shifting lockdown requirements that varied by region.

One of the most interesting lessons from this period is that organizations that had already invested in technologies that enabled secure remote and hybrid work alternatives were in a far better position to transition to a remote-working model. Expanding beyond this type of technology or event allows one to keep up with technological breakthroughs that aid organizational resilience.

Why Resiliency Over Efficiency

Research firm Gartner released a study in 2020 that identified a link between efficiency and fragility.[1] It found that keenly focusing on efficiency can lead your organization down a path that favors tried-and-true methods over innovation that opens new revenue streams and supports long-term success.

As renowned leadership author and speaker Simon Sinek once said, "Innovation is not efficient." It's not going to happen overnight. It's not comfortable. It's slow. True innovation requires trial and error, refinement and dedication to experimentation. Just ask any successful entrepreneur. It's unlikely they discovered their winning idea the first time they sat down to ideate.

Reverse engineering someone else's idea or copying a competitor is easier. Coming up with something new and game-changing is challenging, time-consuming and costly. It is critical to understand the type of organization you currently have and, more significantly, the organization you wish to become.

How to Know if Your Organization Is Original

Go to your favorite search engine and search for your company's category. Look for the first three to five results that aren't yours. Are they using the same language to describe the value of their products or services that you are? If so, consider revising your messaging to home in on relevant differentiators.

4 Hinderances to Organizational Resilience

According to Gartner, these are the four main issues hindering resilience in organizations: misaligned workflows, overwhelmed teams, insufficient resources and process rigidity. Before you make any efforts to improve resiliency in your organization, you must first address these four bottlenecks.

Misaligned Workflows

Workflows can easily get misaligned as your organization changes over time if you don't have a change manager who commits to updating your process documentation. People and technologies come and go, roles change, software vendors launch new features and some activities get automated. Each of these changes can impact workflow alignment. Ensure someone in your organization is committed to updating processes and retraining colleagues as workflows adapt over time.

Overwhelmed Teams

No process can fix *team overwhelm*. Keep track of your staff and what you're trying to accomplish. Determine whether or not it's realistic. If team members frequently report fatigue and burnout due to long hours, rude customers or any other concerns, listen to them and look to resolve their grievances before moving forward.

Insufficient Resources

Having insufficient resources to equip colleagues is equally problematic to team overwhelm. Conduct a resource audit before developing a resilience plan to see if better outcomes could be obtained with simple technology or office supply upgrades.

Rigidity

Having processes is good but making them so rigid that they can't be easily adjusted is bad. The way we work is evolving so rapidly that your processes must be flexible enough to morph to meet new requirements.

We can't stress enough how important it is to address these four concerns before investing in making your organization more resilient. These are the top four impediments to organizational resilience for a reason.

"90% of employees have the skills and mindset to work responsively in a way that promotes organizational resilience, but less than 40% can actively work responsively in day-to-day work."

- Caroline Walsh, VP of Human Resources, Gartner

Save yourself the hassle of focusing on the wrong problem by putting Gartner's research to work for your organization. They did the hard job of figuring out where to focus your attention first, so take advantage of that.

Action Item

Before moving forward with your resiliency planning, stop here and evaluate workflow alignment, team burnout, resource sufficiency and workflow flexibility. Does your organization have any or all of Gartner's four cornerstones of organizational resilience?

The Rise of Hybrid & Remote Work

While we're not out of the woods yet, a few parts of the world are beginning to relax COVID-19 restrictions. Others remain patient, waiting for their turn to once again return to normal. The way we work, socialize and live our everyday lives has changed dramatically over the last year — and businesses are no exception.

With an increasing number of employees working remotely, executives have had to either adapt their recruiting and retention approach or lose top talent to more flexible organizations.

Smart companies have started offering "remote forever" options to reduce the risk of losing talent who might look for a remote job anywhere in the world.

In many ways, our working environments and policies have forever changed. Many think this is a good thing. But regardless of your stance on remote or hybrid work environments, it's becoming necessary for organizations of all sizes to identify long-term plans to support flexible working locations and environments.

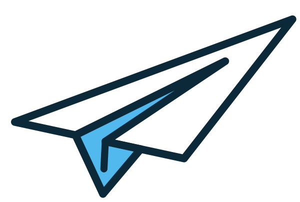
While many organizations staved off such flexibility in the past citing security risks, individuals have tasted the freedom of permanent remote work and many hope to never return to a noisy office after waiting in traffic for an hour or more.

Tapping Into the Global Talent Pool

Urban sprawl has taken on a whole new meaning. Teams that once sat in a single location each day are spread across the country, and in many cases, several countries — an issue that's making 2020 and 2021 tax auditing an absolute nightmare for corporations and auditors as some adventurous employees sought to ride out the pandemic in exotic locations with tax laws much different than their employer's country of origin.

Accounting and Human Resources challenges aside, remote and hybrid work seems to be here to stay, at least for the near future.

As such, organizations must pivot their technology strategies from a survival mode of "remote for now" to a longer-term strategy that supports the need for secure, compliant devices, and platforms and tools that are easy to back up and restore.

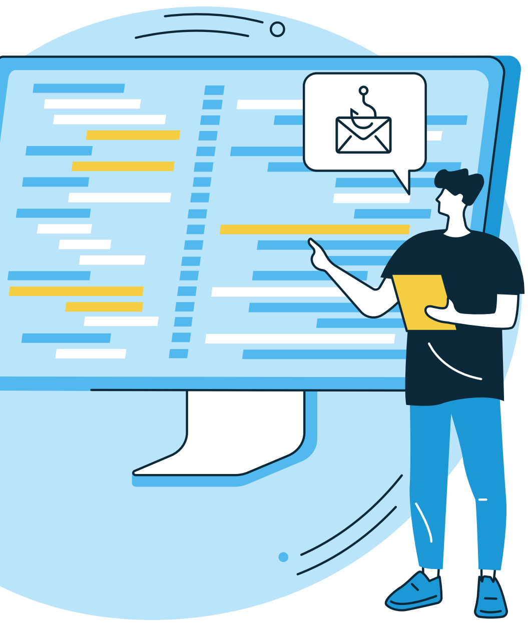


Why the Global Cyberattack Surface Is Expanding

We must acknowledge the growing attack surface without undermining the apparent benefits of hybrid and remote work models. Threat actors exploit often-overlooked vulnerabilities in hybrid and remote work environments. For this reason, organizations should consider adding end-to-end network vulnerability scanning to their cyber resilience strategy.

10 Most Common Cyberattack Vectors Around the Globe

According to a recent briefing from Ponemon[2], these are the most frequently used initial attack vectors to propagate data breaches around the world:



- 20% **Compromised Credentials**
- 17% **Phishing**
- 15% **Cloud Misconfiguration**
- 14% **Vulnerability in Third-party Software**
- 9% **Physical Security Compromise**
- 8% **Malicious Insider**
- 6% **Accidental Data Loss/Lost Device**
- 5% **System Error**
- 4% **Business Email Compromise**
- 2% **Social Engineering**

Cyber Liability Insurance Isn't a Cure-All

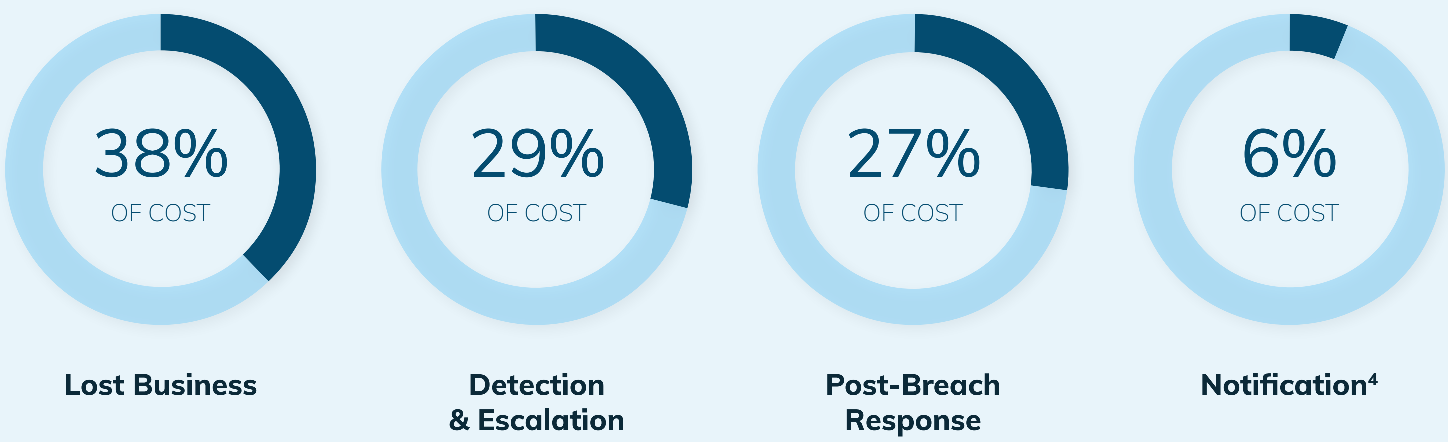
While cyber liability insurance (CLI) might cover an incident, you'll have to prove that your organization has been compliant with its policy terms in order to earn your payout. Scanning for compliance can help you avoid losing a payout in the event of an incident. However, a managed IT service provider (MSP) can help you with this. From GDPR and PHI to HIPAA considerations, an MSP can help you measure and hold accountability to compliance standards relevant to your region and industry.

Personally identifiable information, such as credit card numbers, Social Security numbers, driver's license numbers and healthcare records, as well as company information, customer lists and source code, are all common data breach targets.[3] This has the potential to destroy an organization's reputation in an instant.

Prevention Leads to Better Outcomes

The best outcome, however, when it comes to an expanding attack surface, is prevention. Customer service delays, missed opportunities and reputational damage are all consequences of downtime, even if your insurance policy covers it.

Top 4 Data Breach Costs



Definition:

Cyber Resilience

According to Forrester, "Cyber resiliency is the ability to predict, resist, recover from, and adapt to both adverse and changing business conditions."[5]

6 Keys to Building Cybersecurity Resilience

Improving your organization's cybersecurity posture often entails implementing technologies, frameworks and protocols that reduce the size of the attack surface. The smaller the attack surface, the better. Having an IT network and infrastructure with safeguards in place to identify and prevent the spread of malicious code can go a long way towards bolstering organizational resilience.

Though ransomware is just one of a plethora of growing threats organizations face, one study estimated that the incidents of reported ransomware attacks increased by 300% since the beginning of the COVID-19 pandemic.[6] According to Deloitte, there are six things an organization can do to improve its cybersecurity resilience in the face of an increasingly geographically dispersed workforce and an expanding attack surface:

1

Review & Revise Your Incident Response Plan

At a minimum, conduct an annual review of your incident response plan to ensure it factors in the latest technological and environmental changes that could affect your organization.

2

Enhance Access Management

One in five breaches (20%) are initially caused by compromised credentials.[7] Ensure staff are using two-factor authentication (2FA) across all accounts. This extra step might seem cumbersome, but it helps reduce cybersecurity incidents. For additional layers of defense, consider implementing an identity and access management (IAM) as well as a single-sign-on (SSO) solution to add protection while still making it easy for employees to access their accounts.

3

Improve Cyber Hygiene

"Cyber hygiene (or cybersecurity hygiene) is a cybersecurity practice that maintains the basic health and security of hardware and software. It is a joint precautionary measure performed by an organization's security practitioner, computer system administrator and users to help protect against attacks."[8]

4

Segment & Zone

Flat networks allow infiltrators to move laterally across the network virtually unencumbered. Segmenting your network essentially adds security checkpoints that prevent the unhindered spread of malicious content across your network.

Think of a healthy network like a submarine — each critical area can be sectioned off to prevent the whole vessel from flooding if one area is compromised.

5

Strengthen IT Asset Management

Instead of provisioning and forgetting, ensure measures are put in place to track who has access to which platforms and devices. This makes offboarding assets and employees more effective.

6

Streamline Backups

Excessive backup duplication can actually accelerate the spread of malware through critical systems. To prevent this from happening, consider reverting to the golden rule of backup: three copies, in two locations, and at least one off-site — preferably in a storage vault.[9]

"Ransomware is a favorite malware flavor, and we've seen some groups taking copies of the data prior to triggering the encryption and then using it to further pressure the victim."

– 2021 Data Breach Investigation Report, p. 74

Build a Stronger Brand

"Cyber resilience is more than just a security imperative; it is the foundation of a strong business and brand."[10]

– Forrester

Why Organizational Resilience Matters

Organizational resilience is vital because it equips you to recover from setbacks faster. Regardless of what those setbacks entail, having a resiliency strategy and culture in place helps companies effectively shore up losses and sustain longevity in uncertain times.

Resilient Organizations

- Create an environment for innovation
- Adapt to meet changing customer needs
- Overcome reputational and organizational setbacks
- Rise to the challenge

Tactics of Resilient Organizations

Proactive cybersecurity planning

Depending upon your industry and location, this might entail implementing recommendations from The International Standards Organization (ISO), The British Standards Institute (BSI) or the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, etc.

Protection of Intellectual Property (IP)

More of a legal and operational activity, this includes having proper employee, contractor and partnership agreements in place to prevent disclosure of sensitive organizational IP.

Implementation of uptime safeguards

This entails being able to get back up and running quickly through automatic failover or backup and recovery.

Contingency plan mapping

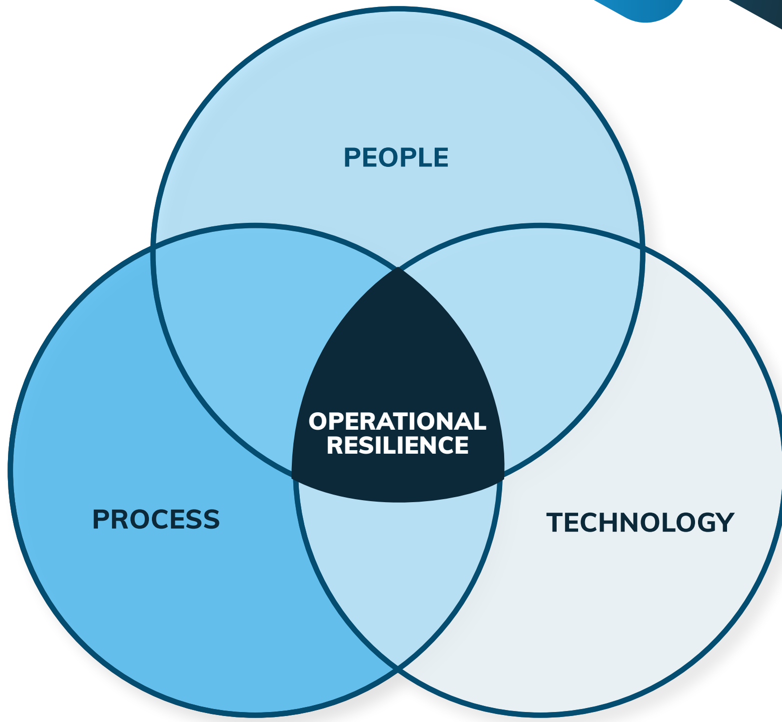
Get ahead of sticky situations by building a business continuity and disaster recovery plan that maps out contingency plans for situations like downtime, evacuations, etc.

Resilience as a Competitive Differentiator

According to Deloitte, resilient organizations are more prepared, adaptable, collaborative, trustworthy and responsible.[11]

What's Included in Organizational Resilience

Three core elements of organizational resilience are People, Process & Technology — in that order. Ideally, processes and technology should bolster employee resilience, making it easy for them to follow effective paths and pivot as needed to ensure the organization is considering new information and market conditions.



People

Building resilience for people means investing in support systems that support mental health and equip employees with tools to avoid or minimize burnout. This is an important part of a sustainable organization. People aren't disposable. In fact, human capital is an organization's greatest asset.

When a tenured team player walks out the door, not only do you lose all the experiential knowledge they brought to the table, but you also risk losing other employees who are left to pick up the slack. Burnout has become such a global challenge for organizations that the World Health Organization (WHO) formally recognizes it as a disease.[12]

The COVID-19 global pandemic has had a significant impact on the global workforce. According to the U.S. Department of Labor, in the months of April through June of 2021 alone, 11.5 million workers quit their jobs.[13] What's been termed "The Great Resignation" doesn't apply just to the United States. Organizations across the world are facing similar challenges. From Gallup Polls to LinkedIn surveys and labor market studies, this trend shows no sign of slowing anytime soon.

Instead of "getting the most out of employees," consider the cost of burnout. According to the HBR, "burnout is an organizational problem, not an individual one."[14] To combat this issue, some U.S. companies are responding to the rapid rise of workplace burnout by providing "wellness weeks" — a week of the organization shutting down to give employees a chance to relax and recharge.[15]

A balanced approach to performance expectations and work-life balance can deliver significantly more value over time, leading to better employee and customer retention. This curbs recruitment costs and helps bolster organizational stability from a revenue standpoint.

4 Ways to Prevent Workplace Burnout & Nurture Resilience

According to research from Gallup, here are four steps any organization can take to curb employee burnout and promote resilience:

Enable managers to proactively look for and address burnout

Managers and colleagues with eyes on team members every week are in the best position to identify signs of burnout. Equip them with the skills and resources needed to address early warning signs and provide relief.

Set clear role expectations and structure jobs

While flexibility for processes and employee schedules is important, so too is structure. Without clear expectations and structure, you'll find employees prioritizing the wrong things, duplicating effort needlessly or simply spinning their wheels. Later on, we'll talk more about the importance of effective change management and how it supports this effort.

Encourage teamwork and shared accountability

Get ahead of siloes of chaos by getting everyone on the same page from the start. This can encourage helpful collaboration and camaraderie, which is the foundation of winning organizational cultures.

Design ideal environments

While this might be more on remote workers amid COVID-19 than employers, organizations can still provide stipends for ergonomic work setups that promote wellness. As employees return to the office, this may mean shifting this approach to providing calmer in-office areas for those who require intense concentration to do their tasks.[16]

Process

Resilient processes are clear, well-researched and take all users and use cases into consideration. They drive organizational effectiveness, are easily adaptable and can easily be documented and taught to others. We'll go over this in greater detail in the section on change management that follows.

To help gauge operational resilience, research firm McKinsey developed the Operations Resilience Index, which "helps pinpoint parts of a company's cost base that are most rigid. Over time, the index provides organizations with a way of tracking their progress and benchmarking themselves even as standards for leadership in flexibility and productivity continue to evolve."[17]

Technology

The final core element is technology, and we'll explain how technology can help bolster organizational resilience in our Tech Acceleration section.

1 Audit

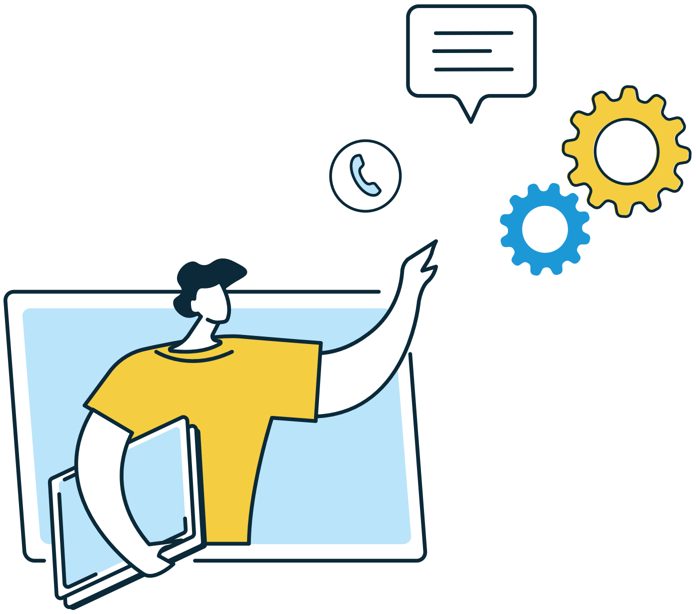
Audit Resilience Gaps

No, we're not talking about taxes here. This pertains to identifying where your organization is struggling from a resilience standpoint. If you're not sure, send employees a quick digital survey (suggest Microsoft Teams for a smaller team or Microsoft Forms for a larger group). This is a good litmus test to begin assessing opportunities for improvement while also engaging your workforce in the problem-solving process.

Depending on the diversity of toolsets and working styles used across your organization, you might find that it makes sense for each department to conduct its own survey. This can be an anonymous survey and include open-ended questions like:

- What's been the biggest challenge at YOUR COMPANY NAME this year?
- What's been your biggest technology or platform challenge this year? How much time would fixing this issue save you each week?
- What do you think makes an organization resilient?
- What do you see as YOUR COMPANY NAME's gaps to being a resilient organization?
- What one change would most impact your personal resilience at YOUR COMPANY NAME?

In all likelihood, your technology team already has a mile-long list of technology issues that a remote workforce brought about. Giving employees outside of the IT team an opportunity to chime in can help you understand what changes could drive immediate improvements for your employees.



Shift Focus to Your Technology Team

Whether your technology team consists of one person, several people or you're just winging it, you can improve resilience outcomes with strategic technology investments. Consider contacting a managed service provider for additional support or evaluation tools to help you make better decisions about whether resilience solutions will give the best return on investment for your organization.

Conduct a Technology Audit

It's really easy during times of crisis to get into "survival mode." Just keeping employees equipped and your business alive could feel like you're biting off more than you can chew. However, continuing to stay in this mode after a crisis has passed can prevent your organization from building resilience. After all, survival and resilience are very different.

As markets grow more stable and predictable, it's critical to assess toolkits, organizational structures, and internal procedures to ensure they're not only relevant, but also supporting security, compliance, and backup best practices, all of which are critical to organizational resilience.

According to TechTarget, an IT audit accomplishes these five tasks[18]:

1. **Evaluates existing systems and processes that secure company data**
2. **Determines risks to a company's information assets**
3. **Identifies methods to minimize data-security risks**
4. **Ensures information management processes are compliant with relevant laws, policies and standards**
5. **Locates inefficiencies in IT systems and system management**

"Organizational resiliency standards, such as ISO and BSI, can prepare organizations for disaster. These questions provide a starting point to validate OR readiness."[19]

– Paul Kirvan, IT Consultant, Auditor & Author, TechTarget

Pro Tip

Organizational resilience doesn't happen overnight. Much like compliance or cybersecurity mastery, it's a practice that requires ongoing evaluation and tuning. The work is never done but the result of the effort can help your organization retain top talent longer and recover from data-loss incidents and other setbacks faster.

Prioritize Technology Gaps to Bridge

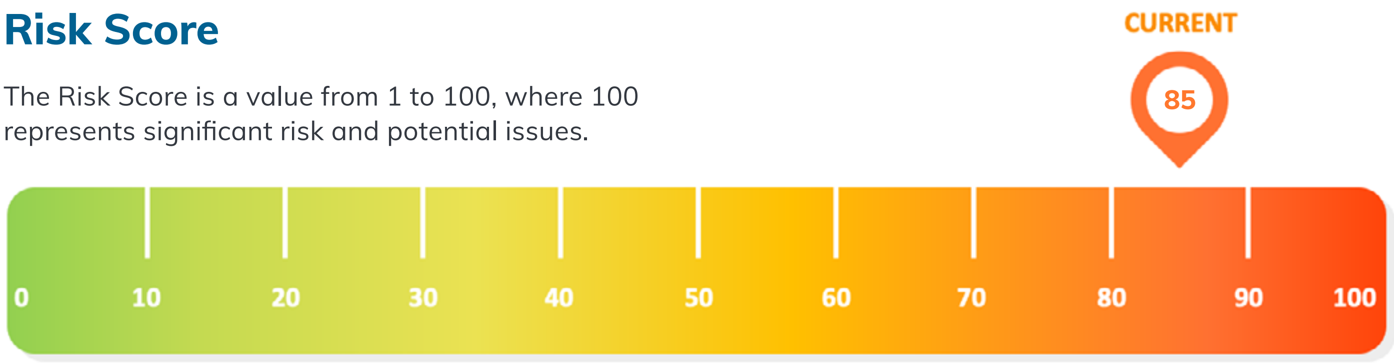
Resilience assessments can seem overwhelming if there's a lot to accomplish. Most technology environments require a fair amount of tuning, routine refreshes and ongoing support to maintain resiliency. Prioritizing tasks based on what's most important, as well as what can help your company improve productivity, customer service or another measure you care about, is a fantastic approach to keep things under control — for both budgets and teams.

Too much change all at once can create unnecessary friction points within your organization, which can result in an increase in costly mistakes, organizational stress and employee or customer churn. To get ahead of these challenges, prioritize and communicate resilience plans, timelines and goals well in advance.

Change takes time. From training people how to use the new technologies to integrating them into existing platforms and documenting new processes, new tech takes time to fully implement and adopt. However, the benefits often outweigh the initial strain.

Risk Score

The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.



Pro Tip

Replacing inflexible, legacy technologies that are either no longer supported or offer poor or no integration with your technology stack is a good way to improve your cyber resilience posture.

Change Management for Resilience

Change is stressful, and ironically, adding new technologies to improve organizational outcomes will cause organizational stress. However, this is just another opportunity to put organizational resilience tenets into practice.

You've probably seen this scenario play out before. Executive management selects and implements new technology designed to improve productivity, but it's implemented at such a breakneck pace that it leads to inevitable workflow glitches and stoppages, which ultimately adds to employee stress, reduces productivity and culminates in top talent walking out the door.

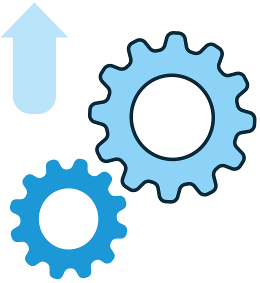
This can be completely avoidable and is an excellent example of why organizational resilience must consider people and technology — in that order.

No matter how far into the weeds we get with technology, automation and the future of work, we must always remember what we're doing is to make life a little easier for employees and customers. This must be the driving force behind technological advancements to ensure long-term success rather than merely short-term gains.

As you look to tried and true frameworks, like Six Sigma, Agile Methodology and other frameworks designed to simplify project and change management, to drive these changes, also be sure to ask:

- How will this impact employees?
- How can we adjust implementation timeframes or practices to minimize stress?
- What feedback loops can we include to ensure colleagues feel heard as we make these changes?

Small perspective shifts like these can help bolster employee resilience and perseverance through meaningful and necessary technology replacements or upgrades.



Accelerate Resilience With Technology

Partnering together on a study, the World Economic Forum and McKinsey found that organizations "often achieve significant and simultaneous improvements in multiple performance measures when they integrate advanced digital technologies across the value chain."[20] Positive outcomes include:

Productivity increase by up to 90%

Energy efficiency improvement of up to 50%

Speed-to-market improvement of up to 100%

Lead time reduction of up to 80%

From cybersecurity to compliance and backup and recovery, an organization's entire technology ecosystem must be considered when implementing a comprehensive organizational resilience strategy. If this seems overwhelming, start with mission-critical tools and applications first.

There is no one-size-fits-all approach to organizational resilience. A managed services provider (MSP) can help you create a custom plan to fit your specific goals and environment.

Why Invest in Resilient Technologies

Investing in resilient technologies — such as infrastructure, security, backup, compliance and managed technology services—across an organization, from the IT team to Human Resources — creates a safety net that can be used to isolate and prevent the spread of malicious behavior, pivot with market conditions or recover more quickly from unexpected setbacks.

Plan to Recover Sustainably, Not Just Quickly

In this digital age where everything moves at the speed of light, it can be tempting to rush through process implementations, technology upgrades and new hire training. But at what cost? Speed without accuracy can cost your organization greatly if it impacts uptime and data privacy, causes compliance issues, or unwittingly lets malicious code slip into your network.

Test, Refine, Document

Take the time to implement resilience technologies and strategies well so that they'll work toward making your organization stronger instead of opening the door to additional vulnerabilities. This means taking time to prototype and test new technologies and resilience strategies before launching them organization-wide.

Then, when your tested solutions are production-ready, ensure an adequate training program is in place for all users as well as a designated change manager who can troubleshoot issues that arise and update documentation as needed to reflect new processes.

Implement a Communications Plan

Have a communications strategy in place so that those affected (internal and external) are aware of the change that's coming and know what steps they'll need to take to be successful using new technology or following a new process.

Don't Forget About Your Supply Chain

If your supply chain becomes corrupted, it could affect your organization if you don't have modern cyber resilience technologies in place to identify, isolate and remediate threats as they arise.

From contractors, outside agencies, and third-party suppliers or fourth-party fulfillers, make sure your supply chain is secure. Before entering into partnerships, put measures in place on your side to identify, block, and/or remediate issues that could be introduced by your supply chain and also ask potential partners about the security solutions they have in place to protect your organization.

Mounting Need for Supply Chain Resilience

The need for resilience in supply chains across industries and organizations across the globe is increasing. In fact, McKinsey found that 90% of supply chain leaders recognize the need for greater resilience. [21]

Back to Basics: Agility

Agility is simply the ability to adapt quickly. When it comes to your technology stack, this might entail selecting solutions designed to work together through integration or a common platform.

Anyone who has worked for more than a few months at an organization understands the frustration of duplicating effort due to systems that should theoretically integrate but don't in practice. Building true agility for resilience means this must be rooted out. Like weeds in a garden, poor integration needs to be addressed rather than ignored until it becomes unbearable.

Commit to Tech Stack Integration

Replace legacy technology systems that simply won't integrate with alternatives. The short-term pain of switching platforms is well worth the long-term productivity as well as employee and customer satisfaction gains.

Trust: The Glue That Makes Teams & Organizations Resilient

Whether you follow the work of Angela Duckworth, Brene Brown or Simon Sinek, you'll find a common theme among their research — trusting teams are not only more resilient but are often capable of accomplishing more. And not just more, but harder tasks.

Though it may sound a bit cliché, research has shown time and again that individuals are capable of completing nearly impossible feats when they have the support of a team they trust.

In the technology space, the most popular reference to anything trust-related is "zero trust." This is fine for IT security protocols, but as we shift our focus to human beings, the approach must change. If you truly want a resilient organization, Brown, Duckworth and Sinek all agree that you must hire for integrity over performance and build a culture that encourages truth-telling.

This is not advocating for brutal honesty, rudeness or intentional harm. Tone, intent and impact definitely matter. But honest feedback can help you avoid costly setbacks — like investing thousands of dollars in a technology stack that's not right for your organization.

Without even doing a Google search, you can probably think of two or more companies that crashed and burned due to groupthink.

Remember, silence can be detrimental to resilience.

The tech space is filled with noise. Just adapting filters so that you can focus on what's important is half the battle won. But, counterintuitive as it may sound, silencing detractors can be problematic. Inviting in and considering many perspectives can help bolster organizational resilience.

But individuals will only share candid feedback if they feel empowered to do so. Consider creating regular feedback loops in your organization so that critical errors or issues can be reported, reviewed and addressed in a timely manner. As the saying goes, "a stitch in time saves nine." The failures of Blockbuster and WeWork certainly illustrate the importance of proactive remediation over knee-jerk recovery efforts.

If trust can drive greater results, lack of trust can drive productivity, loyalty, collaboration and innovation in the opposite direction.

Creating a Culture of Resilience

Nurture trust. Believe it or not, there's a scientific connection between compassion and trust. Health psychologist and Stanford University lecturer Kelly McGonigal suggests that compassion is a predecessor to resilience. A highly competitive, cut-throat environment isn't likely to score high in trust or resilience. So, do the opposite. If organizational resilience is your goal, take the initiative to build your team resilience. Encourage collaboration, encourage compassion and build trusting teams that support each other during difficult times. This is the foundation of resilience.

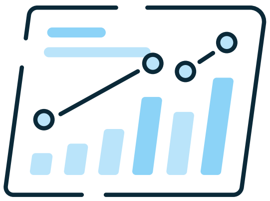
In addition to compassion promoting human resilience, a study from Deloitte that surveyed CXOs found a strong connection between authenticity and organizational resilience.[22] This means that organizations that practice authenticity are more resilient. Therefore, encouraging compassion and authenticity within your organization can actually bolster organizational resilience.

5 Resilience Questions Deloitte Recommends Business Leaders Ponder

- Are we providing a safe environment for our workers?
- Are we instilling ethical principles in our advanced technology?
- Is our supply chain transparent?
- What cybersecurity protections do we have in place to support our customers' and employees' privacy?
- What mental health resources are we providing our employees?[23]

> **"Employers who support their workers — by keeping them physically safe, providing adequate mental health resources and enabling flexible work solutions — are more resilient."[24]**
>
> *– Deloitte*

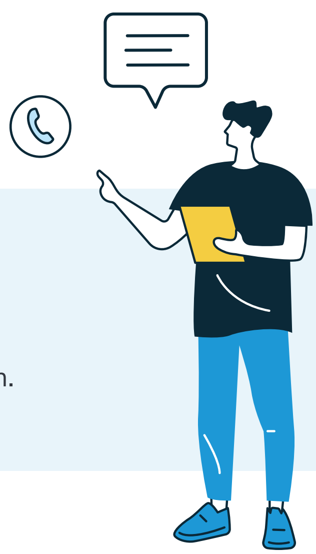
Conclusion



According to BSI, perceived Organizational Resilience across organizations rose globally in 2020, with 33% of surveyed organizations reporting complete confidence in the resilience of their organizations — up 5% from 2019.[25]

Is your organization in the 33% or the 67%? If you're unsure, a managed service provider like us can help you assess your resilience and chart a path forward. Implementing, measuring and holding accountability to these seven building blocks of organizational resilience can mean the difference between short-term versus sustainable success in any industry:

1. **Audit** Resilience Gaps
2. **Prioritize** Technology Gaps to Bridge
3. Practice **Change** Management for Resilience
4. **Accelerate** Resilient Technology
5. Plan to **Recover Sustainably,** Not Just Quickly
6. Stay **Agile**
7. Build **Trust**



Set up a session with us today to get a general technology resilience assessment and/or strengthen the seven building blocks of organizational resilience in your environment. As a managed IT service provider, we have the in-depth, hands-on experience needed to elevate the security and resilience of your technology ecosystem.

SOURCES

1. Gartner.com (Resilience Not Efficiency Will Drive Organizations to Long-Term Success)
2. Ponemon 2021 Cost of a Data Breach Report
3. TechTarget (definition/data-breach)
4. Ponemon 2021 Cost of a Data Breach Report
5. Forrester (Cyber Resilience Study 2021)
6. FBI Internet Crime Complaint Center
7. Ponemon 2021 Cost of a Data Breach Report
8. TechTarget (/definition/cyber-hygiene)
9. Deloitte (Global cyber covid executive briefing)
10. Forrester (Cyber Resilience Study 2021)
11. Deloitte (Global resilience and disruption)
12. WHO (Burnout an occupational phenomenon)
13. Inc.com (The great resignation is here)
14. HBR (Your burnout is unique your recovery will be too)
15. Washingtonpost.com (Employee burnout corporate America)
16. Gallup (Preventing and dealing with employee burnout)
17. McKinsey (Building resilient operations)
18. TechTarget (/definition/IT-audit-information-technology-audit)
19. McKinsey (The need for resiliency)
20. McKinsey (The need for resiliency)
21. McKinsey (The need for resiliency)
22. Building the Resilient Organization: 2021 Deloitte Global Resilience Report
23. Building the Resilient Organization: 2021 Deloitte Global Resilience Report
24. Building the Resilient Organization: 2021 Deloitte Global Resilience Report
25. BSI (Global business leaders confidence in the resilience of their organizations on the rise despite the pandemic)