RSA

3RD EDITION
October 2020

Digital Risk Report

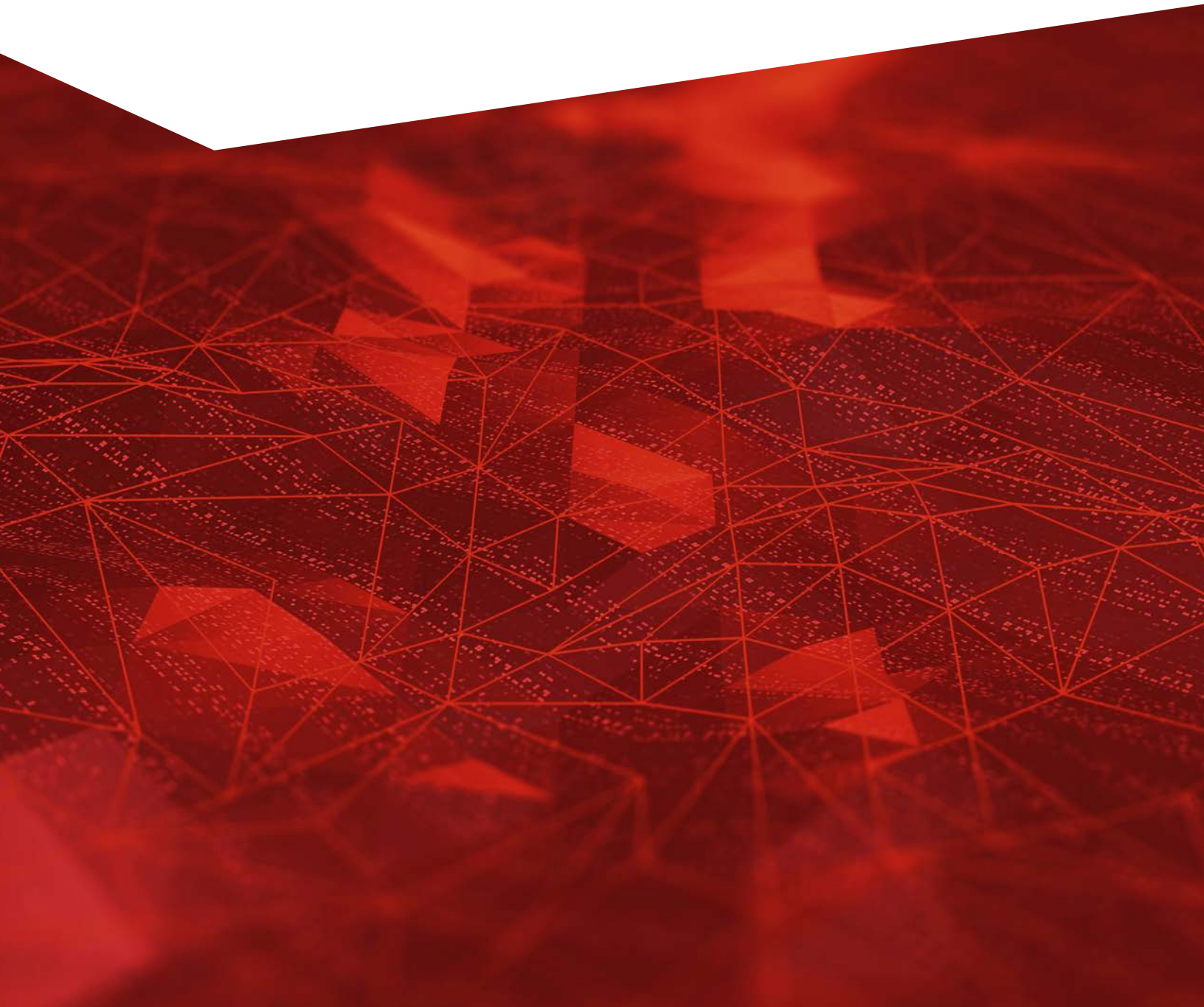


Table of Contents

Managing Risk in the Digital Present

A year of disruption

The pandemic of 2020 without a doubt has had far-reaching consequences. Some industries have been deeply impacted (hospitality, airlines). Others have faced immense challenges to provide essential services (healthcare, government). Some have seen both opportunity and risk in the course of expanding or altering services to meet customer needs (retail, consumer services). All organizations have felt the financial impacts. While some effects have been immediate, drastic and temporary, companies will continue to feel the aftermath of the crisis for some time, ranging from internal financial-priority shifts to industrywide repercussions.

Regardless of their own unique circumstances, organizations across the globe have had to deal with some common challenges.

- **Business operations** were disrupted in countless ways. Customer bases shifted; in some cases they evaporated, while in other cases they multiplied exponentially. Below this massive external force of change, organizations waded through internal phases of dealing with emergency situations to keep the business running. Most organizations enacted continuity and recovery plans at a minimum, in many cases relying on technology to maintain operations. Some organizations had to go into full crisis-management mode.
- The **workforce** faced all kinds of challenges, starting obviously with health and safety. Stay-at-home orders disrupted employees' lives. Organizations with existing remote working requirements shifted operations; organizations with few remote working capabilities had to stand up emergency services. The term "essential worker" took on new meaning. Business processes had to be adjusted to address remote working, furloughs or other disruptions.
- The ripple effect across the globe disrupted **supply chains**. Supply and demand cycles were upset. Companies with global supply chains had to navigate extreme shifts as different regions struggled through the crisis. Some organizations had to find alternative suppliers on the fly or adapt their own production cycles to meet their obligations.
- Finally, the crisis was a **security and risk** "perfect storm." Threats were heightened while business operations were increasingly fragile. Cybercriminals gave no quarter as they ramped up phishing attacks and other scams to exploit already battered organizations. The likelihood of a negative event went up rapidly while the impact increased due to disrupted business operations.

These represent just a sampling of the twists and turns 2020 served up. Pandemics are common scenarios on the risk radar of organizations, but no one envisioned a global pandemic of this magnitude. It has been the greatest curveball in risk management history—shattering expectations of the impact and redefining social, financial and technological futures. It is against this backdrop that organizations must now maneuver. Despite the wide range of digital transformation incarnations in organizations, emerging technologies such as IoT, mobile, social, big data and advanced analytics have undeniably opened many doors for business—doors that especially needed to be opened in 2020, as this year ushered in an even stronger imperative towards digital. We are no longer on the precipice of the "digital future"—it is the *digital present*.

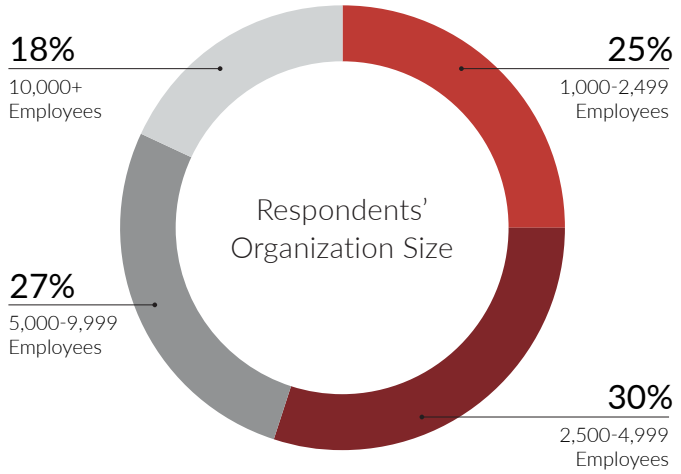
The RSA Digital Risk Survey

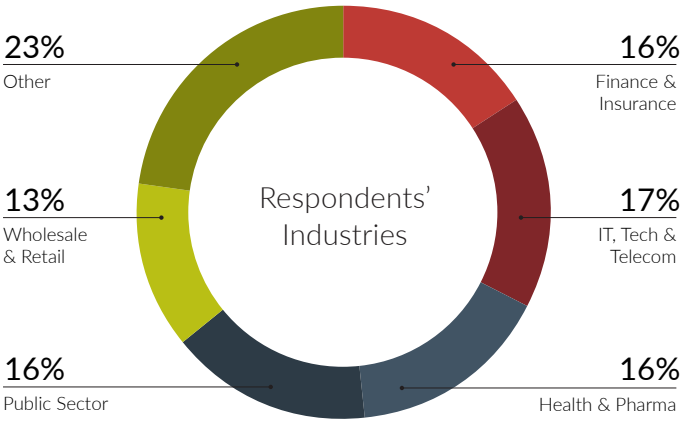
As a leader in the security and risk management industry, RSA is on the front line with our customers as they experience shifts in risk and security management requirements. Suffice to say, the disruptions of 2020 have had a considerable effect on security and risk functions as they balanced priorities to keep the business running and ride waves of change. With heightened urgency to move analog business operations towards digital, challenges continue to cascade across many different risk and security requirements.

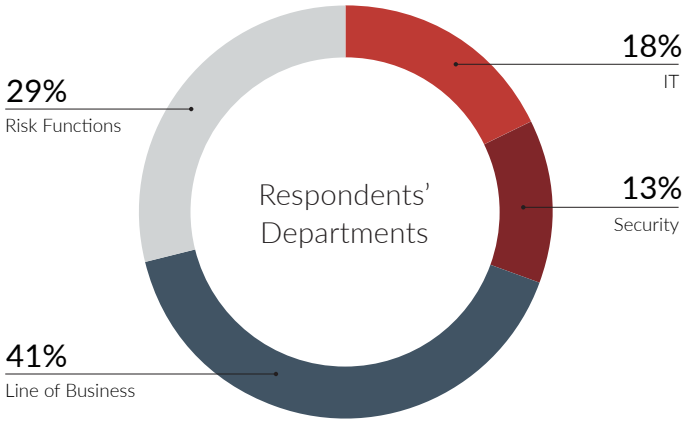
In 2019, we began an effort to better define risk in the era of digital business. To this end, RSA commissioned an independent research firm to conduct surveys to identify the opportunities—and challenges—in the digital world. In our first survey, we uncovered insights into perceptions and priorities from many different practitioners. Over 1,000 respondents completed the double-blind survey last year, across multiple roles, industries and enterprise sizes. This year we used the same methodology with approximately 1,000 respondents. We included several of the same questions so we could see year-over-year changes. We also added some questions to identify shifts in priorities as organizations dealt with the disruptions of the pandemic.

The survey results indicate:

- Existing digital transformation efforts have been critical to maintaining business operations during the disruptions of 2020. The pace of digital initiatives is expected to accelerate focusing on workforce, cloud, and security and risk management.
- Digital risk is hyperconnected—just like the enterprise. There is no easy answer when it comes to priorities. Risk management objectives vary across industries and regions but are evenly spread across different domains, reflecting the need to build a risk and security strategy driven by business objectives.
- As organizations emerge from managing the crises of 2020, a focus on core capabilities that effectively manage intersecting elements of operational risk is essential, with the goal of building true operational resiliency across the enterprise. Collaboration will be key to achieving the goal of a resilient internal and extended enterprise.







On your mark, get set, go

Digital initiatives bolstered organizations' abilities to weather the disruptions of 2020 and as a result the pace of digital business is rapidly accelerating

Last year, cloud initiatives—specifically, moving significant workloads to the cloud—topped the list of types of digital transformation. Other leading types of digital transformation cited in the 2019 survey included extending applications and services to customers, extending the digital footprint to a wider environment and enabling a "work anywhere" workforce. If you consider these priorities in the context of today's environment, these initiatives—especially enabling a "work anywhere" workforce—have proven prescient. For example, entire workforces had to become remote in 2020, and customer-facing applications became very important in many industries as more transactions with customers moved online.

Responses indicated that organizations that had focused on workforce and cloud capabilities were likely better positioned for this year's challenges. When asked, "Which of these (digital initiatives) were most helpful in sustaining your business operations during the current pandemic?" respondents cited "enabling a 'work anywhere' workforce" (36%) and "moving workloads to the cloud" (29%) as the top choices. Those respondents that felt their organization had plans and technologies in place to help manage digital risk during the pandemic cited responding to workforce changes, e.g., providing remote access and remote working infrastructure (64%), as the top capability that helped. These results point to the importance of digital efforts in preparing for future events and support the premise that digitally mature companies are better able to adjust to quickly changing conditions.

In this year's survey, as expected, we continue to see a considerable focus on "work anywhere" and cloud initiatives in the responses to the question about types of digital initiatives organizations have implemented recently. Cloud, workforce and process automation are natural outcomes of organizations addressing the disruptions of 2020 and have traditionally been key digital initiatives. An interesting result from this year's survey came about when the list of possible answers was expanded to include "extending security, risk and anti-fraud initiatives." We added this classification of digital effort to see if it would be singled out as a key initiative.

Which of the following types of digital transformation initiatives has your organization implemented in the past two years? *Select all that apply.*	
Extending **security**, risk, anti-fraud initiatives	49%
Enabling a "work anywhere" **workforce**	47%
Moving a significant number of workloads to **cloud**(s)	45%
Replacing legacy/analog with digital **processes** or technologies	41%
Applying advanced **analytics** techniques (e.g., AI)	39%
Extending applications or services to **customers**	39%
Using **agile** software development	36%
Extending digital **footprint** (e.g., sensors, mobile devices)	36%
Extending applications or services to **partners**	34%
Linking legacy and **IoT** systems together	31%
Implementing **360°** customer management	30%
Setting up always-connected, **sensor**-enabled or location aware technologies	29%
Implementing **robotics**/automation systems	26%

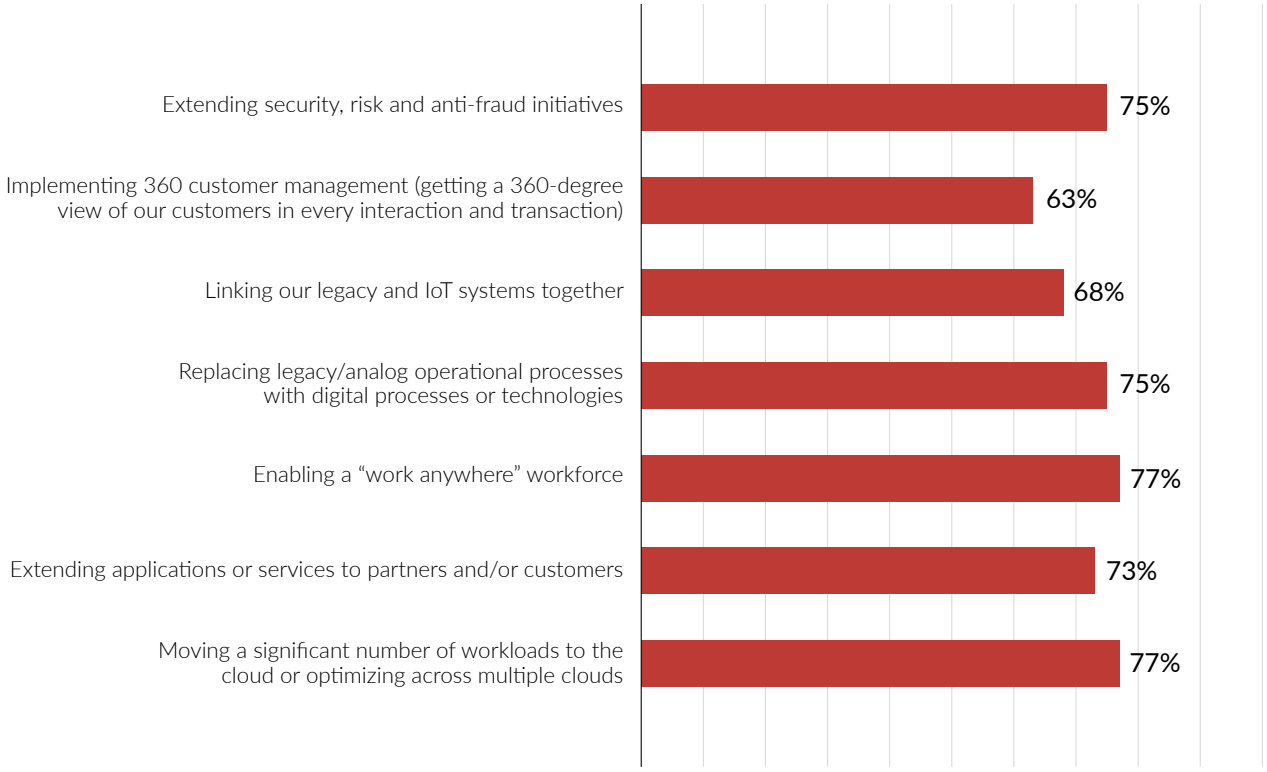
n=980

As it turns out, this new category of digital transformation initiative was the top-ranked response, highlighting that efforts to improve security and risk management have been a central theme within digital transformation. Looking forward, the operational changes that organizations are facing with the "new normal"—such as increased remote workforces, advanced automation and the sophistication of bad actors—will continue to force organizations to focus on risk, security and fraud prevention.

Finally, digital efforts are expected to accelerate, given the experiences of 2020. Nearly 75% of respondents expect their digital initiatives to accelerate. When asked about the acceleration (or deceleration) of individual types of digital initiatives in post-pandemic circumstances, respondents indicated there will be little to no letup on the urgency. Across the top seven types of digital initiatives, 63% to 77% of respondents stated their organizations will accelerate or greatly accelerate efforts.

Figure 1. Respondents Planning to Accelerate Digital Initiatives

Question: "Considering the impact of the current pandemic situation to date, how do you expect your organization will accelerate or decelerate the following types of digital transformation over the next two years?" Percentage of respondents who selected "Will greatly accelerate" or "Will accelerate to some extent." (n=1000)



Hyperconnected risk

Risk related to digital business is extremely intertwined, leading to difficult decisions about priorities

In 2019, over 80% of respondents indicated an expectation that their organization's risk profile would increase or greatly increase. This year's survey reflects much the same sentiment. While 75% of respondents stated their organization's risk profile will expand somewhat or significantly over the next two years, 20% expect risk profiles to remain the same. The drop between 2019 (80%) and 2020 (75%) could possibly be attributed to maturity or comfort levels in digital transformation efforts. However, the point is clear that only a very small percentage of respondents in 2020 (7%) expects risk levels to diminish.

Last year, cybersecurity risk was the clear leader when respondents chose the priority objectives for risk management related to digital initiatives. Obviously, data breaches and disruptions caused by attacks such as phishing and ransomware are serious topics. The associated costs—both financial and reputational—are significant. The ability to detect and respond to attacks is getting more difficult, especially as the threat landscape continues to evolve and reliance on technology increases, thus driving the focus on cybersecurity reflected in last year's survey.

In 2020, attackers continue to advance and use sophisticated techniques to infiltrate organizations, especially during times of massive disruption. With the increase in remote working, organizations no longer have well-defined perimeters, and the pandemic has fueled an increase in phishing attacks that utilize the crisis as a trigger for the attack. The good news is that 76% of respondents stated they had plans and effective technologies in place that helped manage digital risk. Unfortunately, some organizations struggled to adapt in these times of change. One in five respondents indicated their organizations dealt with the pandemic's impact as best they could but were mostly reactive. Respondents that noted their organization had issues with addressing pandemic-related situations cited adjusting security monitoring and controls to shifts in user behavior as the greatest challenge (46%). In addition, ensuring business continuity, disaster recovery and/or crisis response (45%), and responding to workforce changes (42%) were cited heavily as well.

Figure 2. Expected Change to Risk Profile

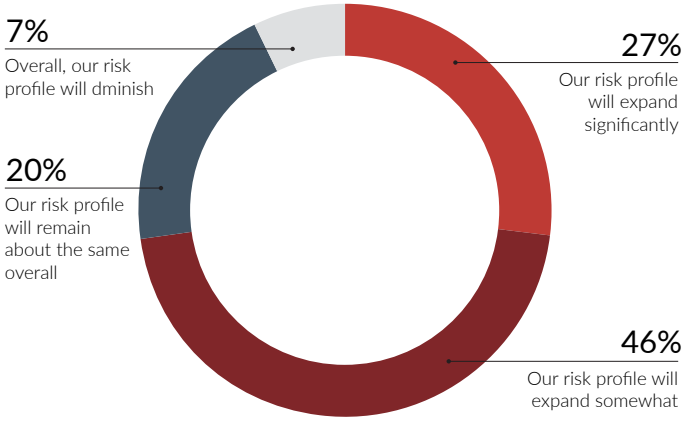
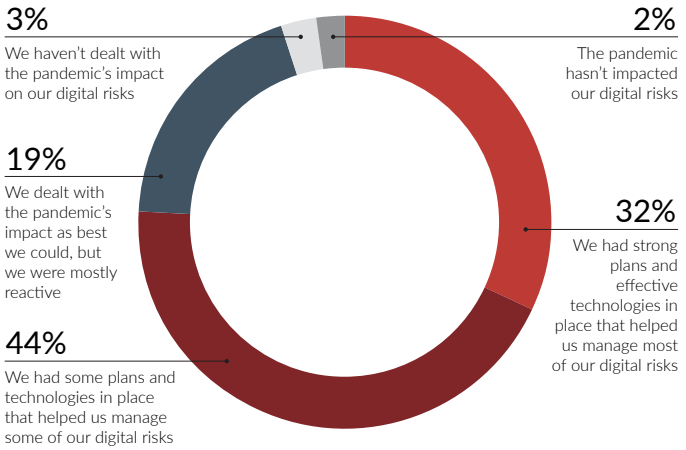


Figure 3. Impact of Pandemic on Digital Risk



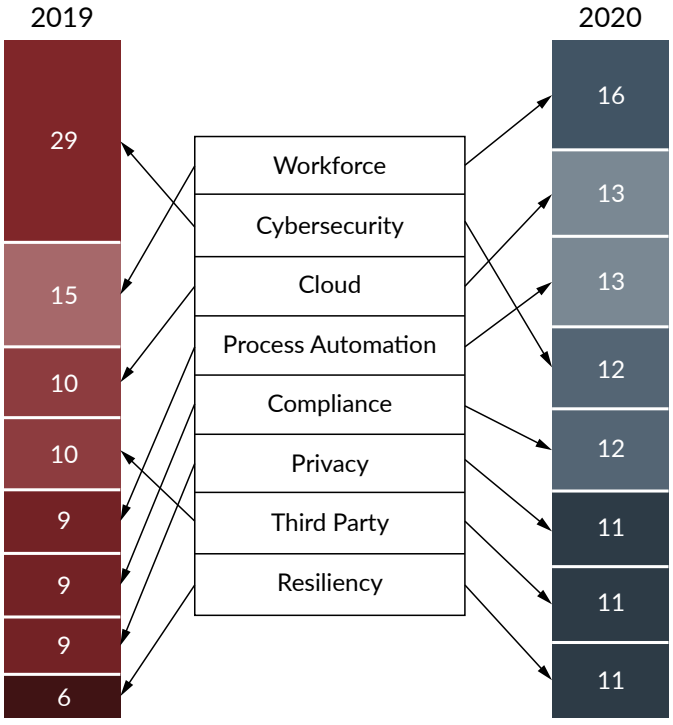
Last year, a key point was that each risk area posed in the survey was selected as someone's #1 priority—meaning cyber attack risk was not the only primary issue for many organizations. Depending on the nature of the organization's digital transformation, other areas such as workforce, third-party risk, cloud, privacy, compliance and resiliency could have been a top priority. We interpreted this as an indicator that priorities were driven mainly by the understandable concern of cyber attack, but also by the nature of the company's digital strategy.

This year, organizations must not only think about the risks that may arise from their digital transformations, but also reconsider which risks are most important for them to manage or mitigate due to the pandemic. In response, risks associated with a dynamic workforce supplanted cyber attack risk as the top-ranked objective in this year's survey. That is understandable, given most organizations had to rely on remote workforces due to the pandemic, and many are accelerating their plans to retain larger numbers of remote workers.

Interestingly, this year's results imply a more nuanced understanding of risk related to digital initiatives. The priority assigned to different types of risk management objectives was more evenly split, as noted in figure 4. Cyber attack risk was a clear leader last year and could be construed as "the easy answer"—meaning that when asked about risks related to digital initiatives, respondents most prominently cited cyber attack risk. However, this year, we see more emphasis on objectives around process automation, cloud and compliance. Compliance rose in priority relative to the other objectives, perhaps hinting at regulatory fallout expected from this year's pandemic.

Figure 4. Changes in Digital Risk Management Objectives

Question: Please think about your organization's strategy to manage the risks that may emerge or increase due to your digital transformation over the next two years. What do you believe will be your organization's most important objectives? (One answer selected; responses in terms of %.)



In short, the risk management objectives related to digital initiatives need to be driven by the business objectives. There is no easy answer. Many of these types of risks overlap—a cyber attack could be a cloud issue, a compliance issue, a privacy issue, involve a third party and so on. Our takeaway is that the even split of priorities highlights the need to think of digital risk as extremely connected, requiring an integrated approach to solutions.

Respondents that indicated their companies had higher levels of digital transformation and risk management maturity were expectedly better prepared in responding to the pandemic.

- Eighty-five percent of respondents whose organizations are extensively engaged in digital transformation efforts felt their organization had plans and technologies in place to manage digital risk during the disruption. Among these respondents, the ability to respond to workforce changes and ensure business continuity were keys to managing risk.
- One-third of respondents reporting early-stage digital transformation felt their organization dealt with the pandemic's impact as best as they could, but were mostly reactive.
- Seventy-nine percent of respondents who described their governance, risk and compliance (GRC) program in mature terms felt their organization had plans and effective technologies in place that helped manage most of their digital risks.
- Of respondents whose companies have implemented basic access management controls such as password management and single sign-on (SSO), and were mainly reactive in their pandemic response, 51% cited responding to workforce changes as their biggest challenge when responding to the pandemic.
- For those respondents who stated their organization has been challenged to manage its digital risks during the current pandemic situation and cited adjusting security monitoring and controls to shifts in user behavior as their biggest challenge, 80% did not have an advanced security operations center (SOC) to detect and respond to threats across multiple domains.

No time like the present

Get back to basics

Fundamental processes to identify, analyze and treat risks must be strengthened and optimized to evaluate priorities

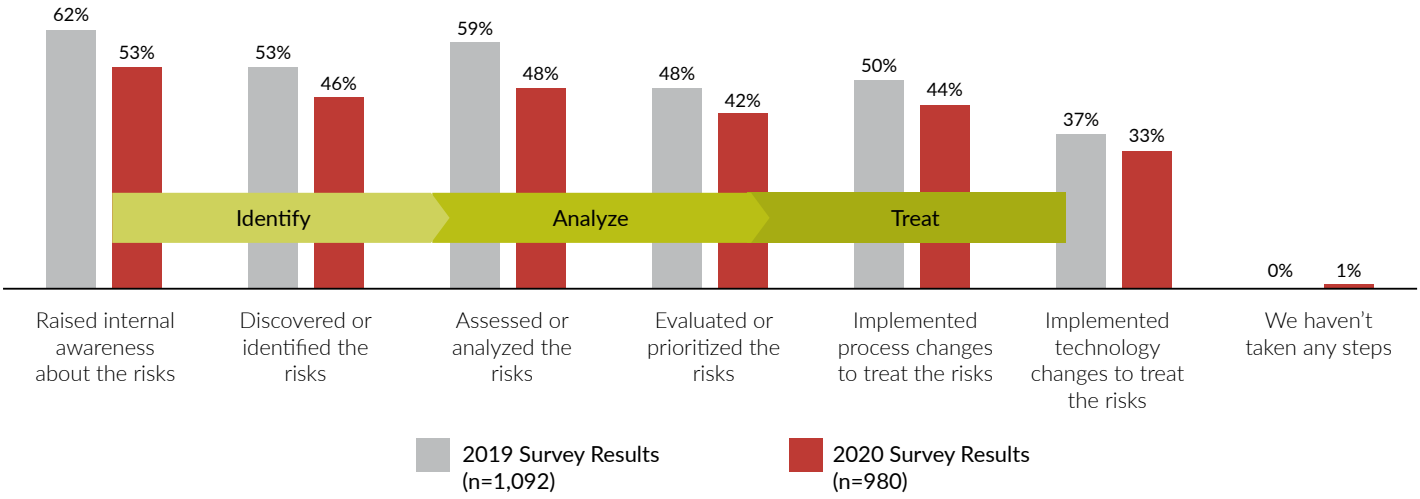
While digital initiatives have already impacted organizations at fundamental levels with a wide range of benefits, the pandemic has applied increasing pressure to be resilient in the face of any disruption. As highlighted previously, respondents that indicated their companies have already reached a level of digital maturity were better positioned to deal with the crisis. Now, there is not only momentum towards digital operations (i.e., customers and employees being more accepting of digital solutions), but also an even more fundamental need to accelerate efforts. The expectations indicated in our survey and in conversations with customers show organizations focusing on four key areas.

1. **Automate business operations:** Examples across the board show where digitally mature companies weathered the storm of the crisis. Retailers continued serving customers through increased online order and pickup services. Manufacturers were able to deal with staffing shortages and rely on automated production. As back-end office functions lean harder on technologies such as videoconferencing and automated workflows to maintain continuity of operations, business operations are on a trajectory to become even more reliant on technology. Therefore, the mantra of "bend, but don't break" is becoming a core element of risk and security strategies. Automation across business operations increases resiliency but also creates a hyperconnected risk environment.
2. **Enable the workforce:** Companies with existing remote capabilities to support operations were able to weather stay-at-home orders more easily and those that had already enabled a dynamic work environment were able to shift operations more quickly. As evidenced in the priority given to workforce-related topics in survey responses, technology will continue to address workforce-facing services—from staff hiring/onboarding to routine meetings—and remote workforces are here to stay. The impact to risk management and security is a more widely dispersed technology footprint and an extremely dynamic user and device catalog. These ingredients add up to challenges in maintaining visibility into threats as well as meeting the operational need to provide secure, frictionless access to data and systems.
3. **Optimize the supply chain:** Advanced analytics and automated supply chains allow organizations to adjust to rapidly shifting supply chain needs. The pandemic underscored the importance of knowing the "who, what, where, why and how" of business ecosystems. The scope of disruption provided vivid clarity on the extent of interdependencies with third parties and the need to rely on a durable ecosystem. In anticipation of disruptions based on geography, automated vendor management processes could make the difference in areas such as prioritizing supply chain issues or fast-tracking assessments of new vendors.
4. **Modernize security and risk management:** Companies with strong security operations (e.g., agile, automated, high visibility) and automated risk management processes (e.g., automated risk assessments, control exception management) can more effectively adjust to emerging risks. Keeping pace with an accelerated digital enterprise has wide-ranging implications for risk functions, such as making process improvements, upskilling security and risk teams, and investing in technology to enhance productivity and effectiveness. However, in trying times and economic

uncertainty, an increased assessment of value for all strategic initiatives is critical. Security and risk teams must look to balance cost, value and risk with credible business cases for technology investment so that they can not only manage risk effectively but also ensure clear strategic benefits.

To manage the risks related to these efforts, the fundamental risk management process has to be stable, defined and ingrained in the thinking of the business. The 2020 survey results indicate an interruption in the process of methodically managing digital risk. There were lower levels of respondents taking steps toward managing digital risk in the traditional "Identify, Analyze and Treat" methods. This could be due to the disruptions that rippled across organizations, distracting security and risk teams from these basic steps. When it comes to prioritizing efforts, the process must work effectively to identify business impacts and foster an understanding of the requirements to reduce risk. Getting back to the basics of risk management helps shape the strategy and align efforts with business objectives.

Figure 5. Steps Taken to Manage Digital Risks



Target high impact capabilities

Efforts must deliver business value while establishing a strong foundation for sustainable and agile risk and security functions

Respondents were asked to prioritize capabilities within the different domains of digital risk management. While not an exhaustive list for each sector of risk and security, the results give insight into key areas of focus. The following are the top capabilities identified within each risk domain.

Key priorities per risk domain based on respondents:

Risk Domain	Top Priorities
Workforce	Risk-based authentication that considers signals associated with user behavior, device security, threat intelligence and fraud
	Multi-factor and passwordless authentication solutions for identity assurance
Cloud	Visibility and insight into cloud controls, including resource policies, configurations and settings
	Risk-based authentication for cloud user identity assurance
Process Automation	Risk management expertise applied to the design and management of advanced process automation
	Network visibility and security controls to manage the risks that may be introduced through the automated processes
Cyber Attack	Threat detection and response
	Coordinated breach response plan across IT, security, business and operations teams
Compliance	Continuous controls monitoring
	Risk-based compliance methodology
Resiliency	Pandemic planning and recovery tools
	Uniform IT disaster recovery and business continuity planning
Third Party	Integrated third-party risk and enterprise risk management approaches
	Risk management of breaches that may be caused by third parties' security lapses or vulnerabilities
Privacy	Assessing privacy risk, including data privacy impact assessments (DPIA)
	Applying technical and organizational privacy-related controls

Collectively, many of these capabilities represent core elements of solid risk and security practices:

- Strong authentication and access control
- Broad visibility into the technology infrastructure to identify security threats
- Integrated approaches to risk and compliance
- Continuous monitoring of controls
- Coordinated processes across functions

This further supports the premise of getting back to basics, as these priorities represent high-value foundational elements for strong security and risk programs.

In addition, respondents were asked questions regarding maturity levels in GRC, security and identity management, along with priorities in the next two years. Highlights from the survey include:

- Seventy-nine percent of respondents expect to rely more heavily on the IT and security risk management portions of their GRC programs over the next two years to manage risk. Other areas of emphasis included data governance (70%), compliance (68%), audit management (64%) and operational risk management (64%). Furthermore, respondents indicated an expectation to heavily prioritize IT and security risk management elements of their GRC programs, regardless of the maturity of those programs. For a second priority, companies with lower maturity of their GRC programs cited data governance and privacy, business continuity and compliance, while companies with higher maturity GRC programs stressed data governance and privacy.
- Fifty-one percent of respondents chose either "We implement detection and response capabilities just enough to meet our compliance requirements" or "We have basic controls in place to block threats, such as anti-malware" to describe their threat detection and response capabilities. These are very low bars considering the significant threat to digital business and the priority of managing cyber attack risk. Given that almost half of respondents were in this state, improvements must be made to threat detection and response.
- Fifty-eight percent of respondents indicated a heavier reliance on network detection and response to manage risk over the next two years. Even respondents who described their security operations as mature indicated a priority in this area, with 69% of respondents in this category indicating they will rely much more or somewhat more on network detection and response.
- Only one in four respondents stated their organizations have implemented access management controls including two-factor or multi-factor authentication for all or almost all applications. Twenty-seven percent have implemented basic access management controls such as password management and SSO, with 46% of respondents stating their organizations have implemented access management controls including two-factor or multi-factor authentication for only the most sensitive applications.

When looking across these findings, three core capabilities become apparent.

1. **Integrated risk management** will become increasingly essential in the coming years and must be positioned to address a continuous cycle of emerging risks. Companies should focus on transitioning to continuous monitoring of controls to improve effectiveness and reduce the cost of compliance. In addition, establishing risk-based approaches applies across the different domains and will advance compliance, business continuity/disaster recovery, security and third-party risk management efforts.

2. **Network detection and response** are paramount to protect the expanding digital enterprise. Compliance and basic controls are not the endgame for security teams. With the extension of remote workforces and accelerated automation indicated by the survey, managing security threats will play a key role in achieving operational resiliency. Advanced security operations are the hub of managing emerging technical security threats.
3. **Identity and access management** will continue to grow in importance as business applications—the backbone of digital operations—move to the cloud or extend across environments with increased remote access. Minimal controls such as password management and SSO with no enhanced authentication or access controls will not address the increased risk. Therefore, moving towards concepts such as "zero trust" when it comes to access management and advanced authentication across all applications must be part of the digital strategy.

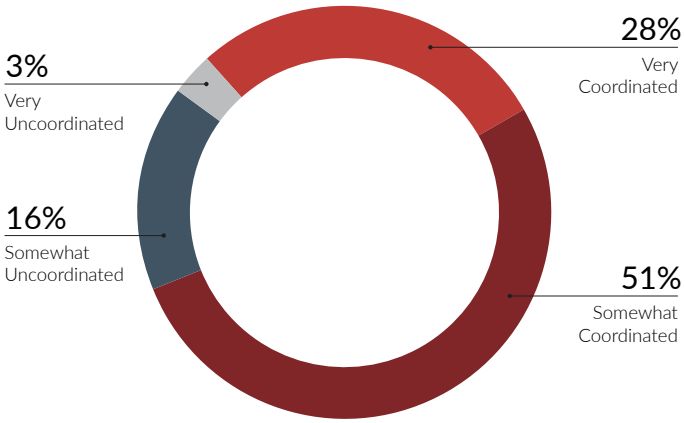
Collaborate and coordinate

Coordination between risk and security functions and alignment with the business is critical for success

The final recommendation coming from the survey results supports a trend RSA has been witnessing and evangelizing for some time. Collaboration across different domains of risk and security management is a key element of building a sustainable, effective program. The survey highlighted one major result of the pandemic—the increased emphasis to improve collaboration between security and risk teams. For purposes of the survey, "risk teams" included risk management, compliance, audit and legal teams to represent an array of internal teams whose focus is on identifying potential obstacles to business objectives.

We asked respondents this year: "To what extent do you believe your security and risk teams worked together in 2019, prior to the pandemic?" The results indicated a solid level of coordination: 28% stated "very coordinated;" 51% stated "somewhat coordinated." This aligns with results of the 2019 survey, in which almost nine out of ten respondents agreed that security and risk teams need to work together to effectively manage the risks that may emerge or increase due to their organization's digital transformation. The 2020 survey gives an indicator on how well that was working. Overall, 79% of respondents stated efforts were somewhat or very coordinated. While leaving room for improvement, this was a positive indicator that the collaboration desired was progressing.

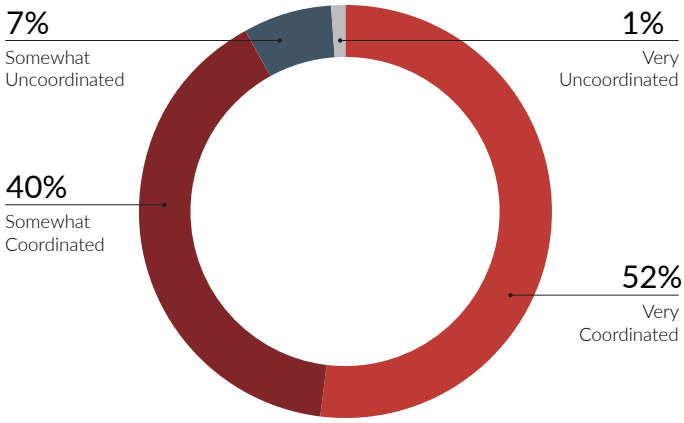
Figure 6. Level of Coordination Between Risk and Security Teams (2019)



This year's survey also indicated the pandemic has created an increased sense of urgency, though. When asked, "To what extent do you believe security and risk teams will work together over the next two years, due to the impact of the pandemic?" a resounding 92% indicated the expectation that those groups would work in a more coordinated fashion.

Additionally, organizations that had higher maturity levels in GRC and threat detection and response indicated a very coordinated effort in the coming years. This is expected, as those organizations have already focused on integrated approaches. Companies with low maturity, though, also expect a much higher level of coordination, indicated by a 30% jump in respondents choosing "very coordinated" as their answer. In short, it isn't just the mature risk and security functions that expect more coordination. This is a universal expectation. Whether it comes to fruition will be a test of time, but the shift towards collaborative efforts is certainly evidenced.

Figure 7. Plans for Coordination Between Risk and Security Teams (next 2 years)



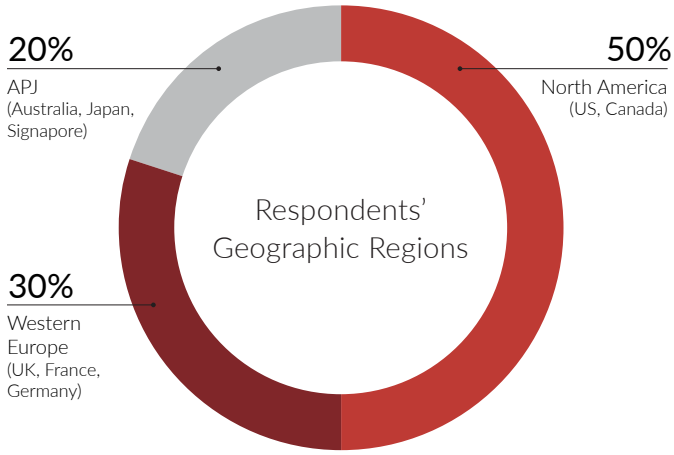
Resiliency in the digital present

While some organizations have completely transformed their businesses with digitally driven products and services, many are still adopting technologies to innovate, optimize operations and unlock value. 2020 has proven to be an unprecedented year of disruption that underscores this imperative. Digitally mature companies—i.e., those that could transition to remote workforces, rely on automated business operations, or transition to products and services delivered to their customers digitally—had a considerable edge as the world faced an extraordinary challenge.

The acceleration of digital transformation will require security and risk functions to equally pick up speed. Keeping pace with digital initiatives related to workforce, cloud and process automation is expected to also require efforts to modernize security and risk management. Addressing the hyperconnected nature of digital risk requires priorities to be aligned with business objectives. Capabilities that shore up the basics, deliver high-value outcomes and reflect the changing technology landscape within organizations will position them for the future. Resiliency in the face of disruption—whether it is a natural disaster, another pandemic or a competitive industry shift—requires discipline and collaboration across the enterprise. The digital present is upon us.

Regional Perspectives: Managing Risk During the Pandemic

RSA's research partner conducted the 2020 RSA Digital Risk Survey in three geographic regions, as shown in figure 8. The respondents held a range of titles across IT, security, risk and other lines of business. To qualify for the survey, respondents had to be working full-time at management levels or higher, at organizations that were involved in or planning digital transformations.

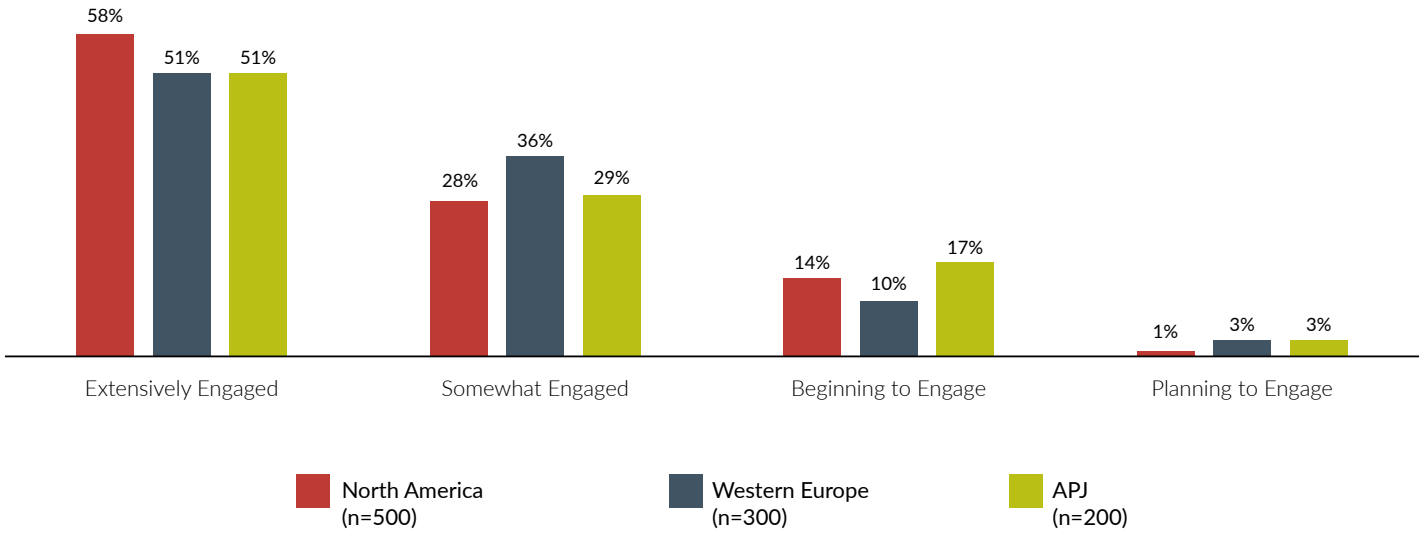


The value of transformation

Digital transformation helps sustain businesses around the world during major disruptions

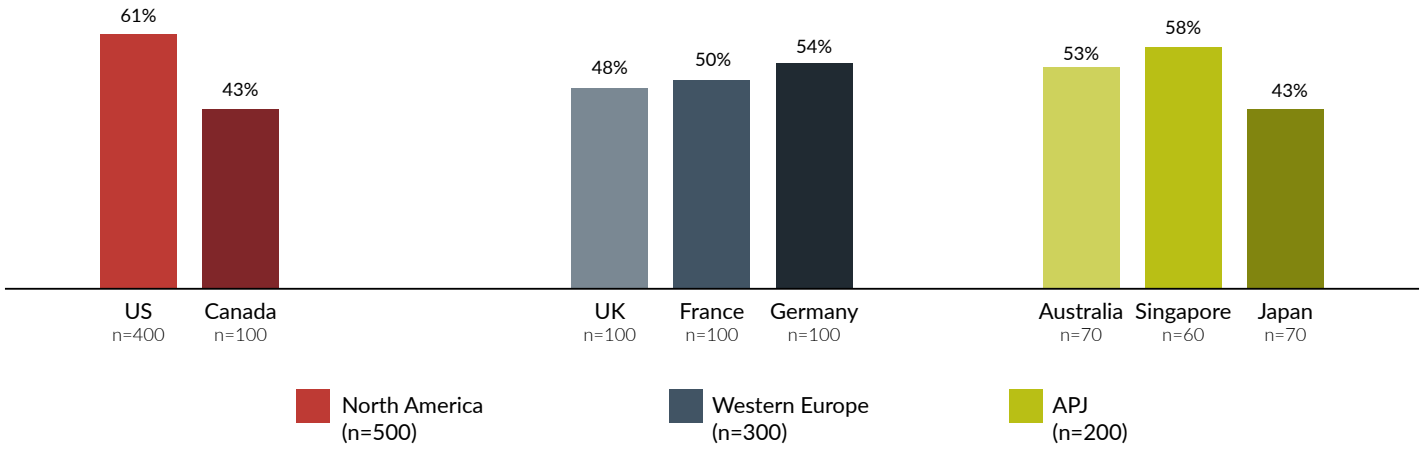
To lay a foundation for understanding the state of digital risk in different geographic regions in the time of pandemic, we first asked respondents about their organizations' level of digital transformation activities. As shown in figure 8, organizations in North America are the most engaged, while many organizations in APJ are still in the planning stages.

Figure 8. Engagement in Digital Transformation, by Region



The level of engagement also varies within each region, as shown in figure 9. In North America, organizations in the US are more extensively engaged; in Western Europe, organizations in Germany are more extensively engaged; and in APJ, organizations in Singapore are more extensively engaged.

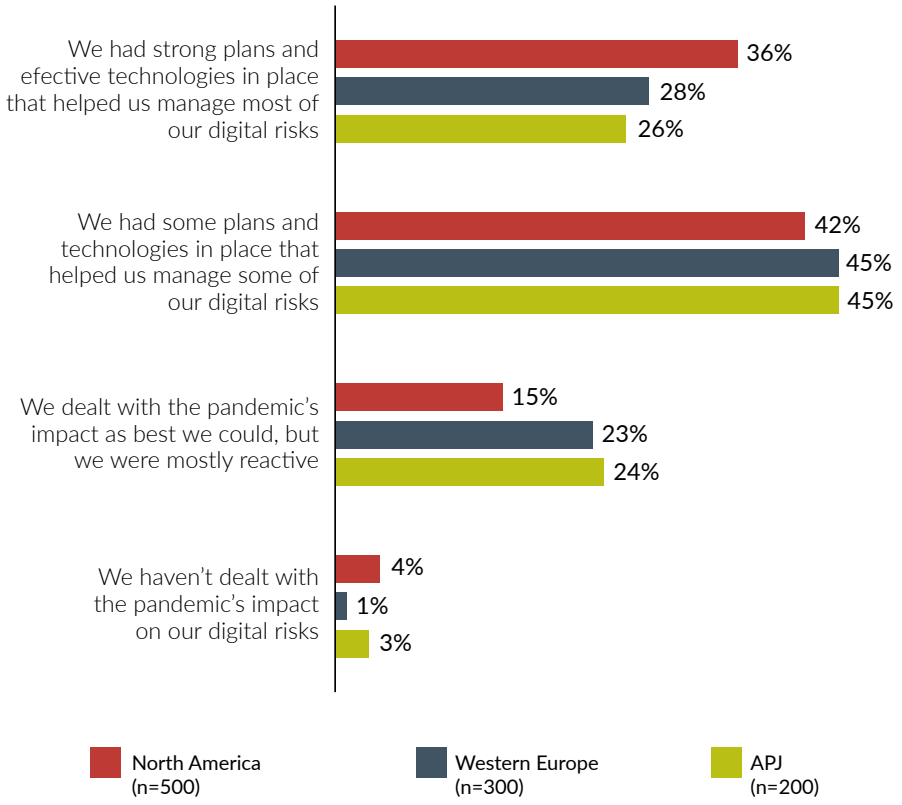
Figure 9. Organizations Extensively Engaged in Digital Transformation, by Country



Next we asked respondents how well their organizations were managing digital risk during the pandemic. As shown in figure 10, respondents in North America were most likely to report that their organizations were managing well, because they had strong plans and effective technologies in place. Respondents in APJ were more likely to say their organizations were not managing as well, either being reactive or not really managing the risk situation at all.

These findings indicate that regions where organizations are already engaged in digital transformations, and already have plans and processes in place to manage any risks that may be associated with their digital operations, are best able to sustain their business operations during a time of crisis such as the current pandemic.

Figure 10. Managing Risks During Pandemic, by Region



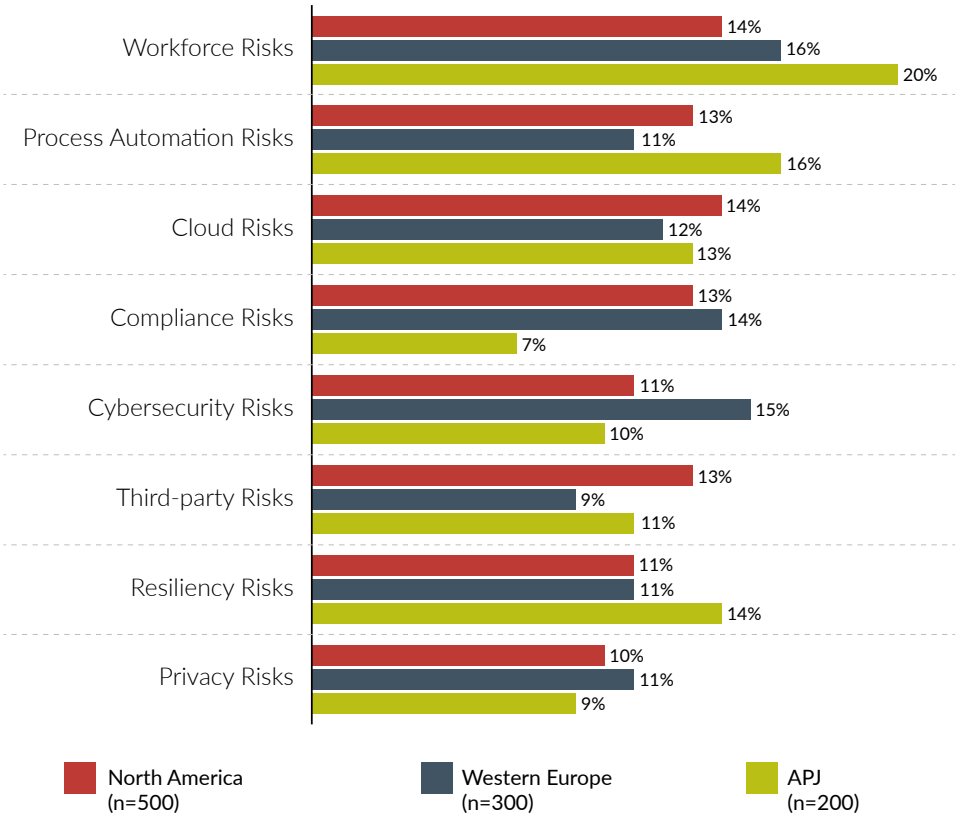
It's not too late to start putting more plans and processes in place as the current pandemic continues. Future disruptions are always on the horizon, and business decision-makers can take the learnings from RSA's 2020 Digital Risk Survey to adopt best practices, described later in this report, for managing risks in the future.

Regional priorities

Organizations are focused on different risk management priorities, depending on their location

The pandemic has had a ripple effect on the risk profiles of organizations around the world, but the impacts are being felt differently depending on where the organization is located. Survey respondents were asked about their organization's top risk management objectives. Figure 11 shows their top-ranked digital risk management objectives.

Figure 11. Top Digital Risk Management Objectives



Organizations in APJ are most concerned about risks associated with their workforces, automated processes and business resiliency. This ties back to the level of difficulty that respondents in APJ reported when asked how their organizations were managing their digital risks (figure 4). Enabling a dynamic workforce, automating processes and ensuring business resiliency are key to sustaining business operations during the pandemic, so this is where organizations in APJ are focused to strengthen their digital risk management strategies going forward.

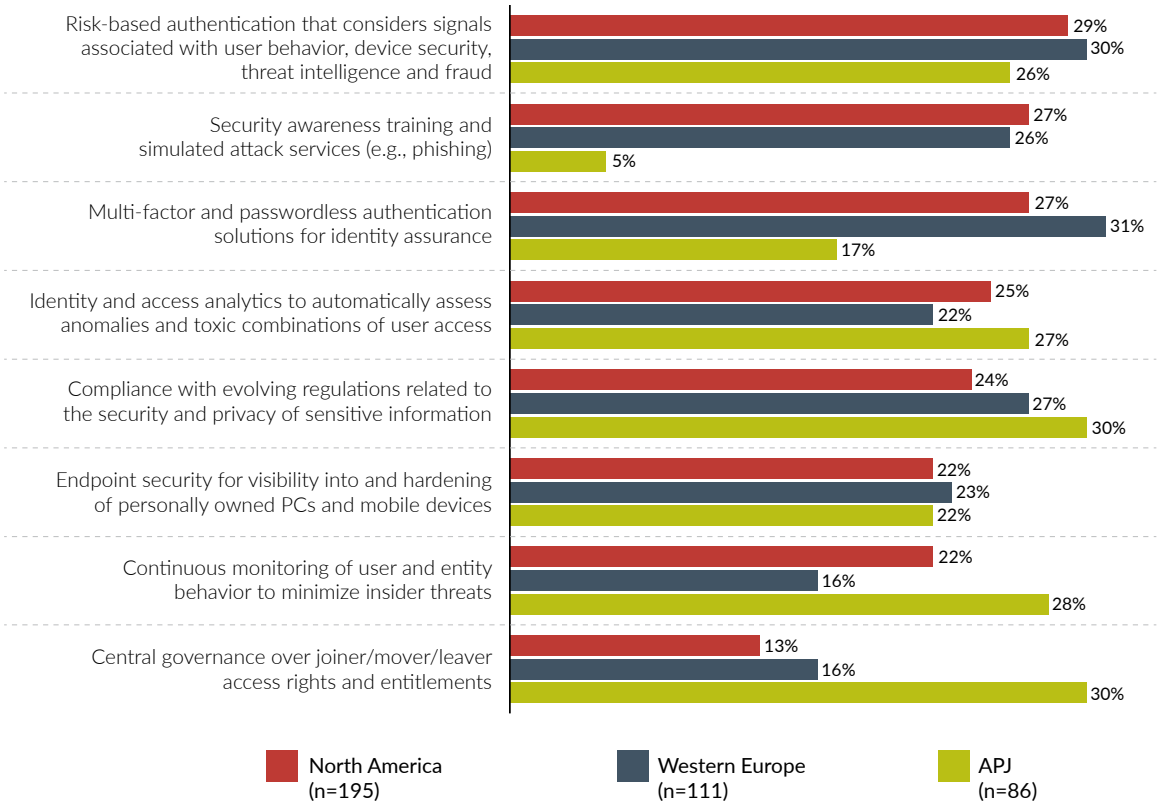
Translating priorities into action

Power the dynamic workforce

As detailed in figure 10, some organizations reported they've been successful in managing their risks during the pandemic, because they already had strong plans and effective technologies in place. We asked respondents from these organizations to select the specific area in which they've been best able to manage their risks. Responding to workforce changes, such as providing remote access and remote working infrastructure, emerged as the top area of success.

There are many technologies that organizations can implement to manage risks that may be associated with their dynamic workforces. When asked which relevant technologies will be most important to their organizations over the next two years, respondents gave answers (figure 12) that provide a roadmap for all organizations to prioritize their workforce risk management implementations within their own region's risk environment.

Figure 12. Planned Technologies to Address Workforce Risks



Organizations in North America and Western Europe plan to focus on multi-factor, risk-based authentication as well as security awareness training as they continue to address risks related to their dynamic workforces. Organizations in APJ will rely on workforce management technologies that are up-to-date with evolving compliance and privacy rules while also providing robust central governance capabilities.

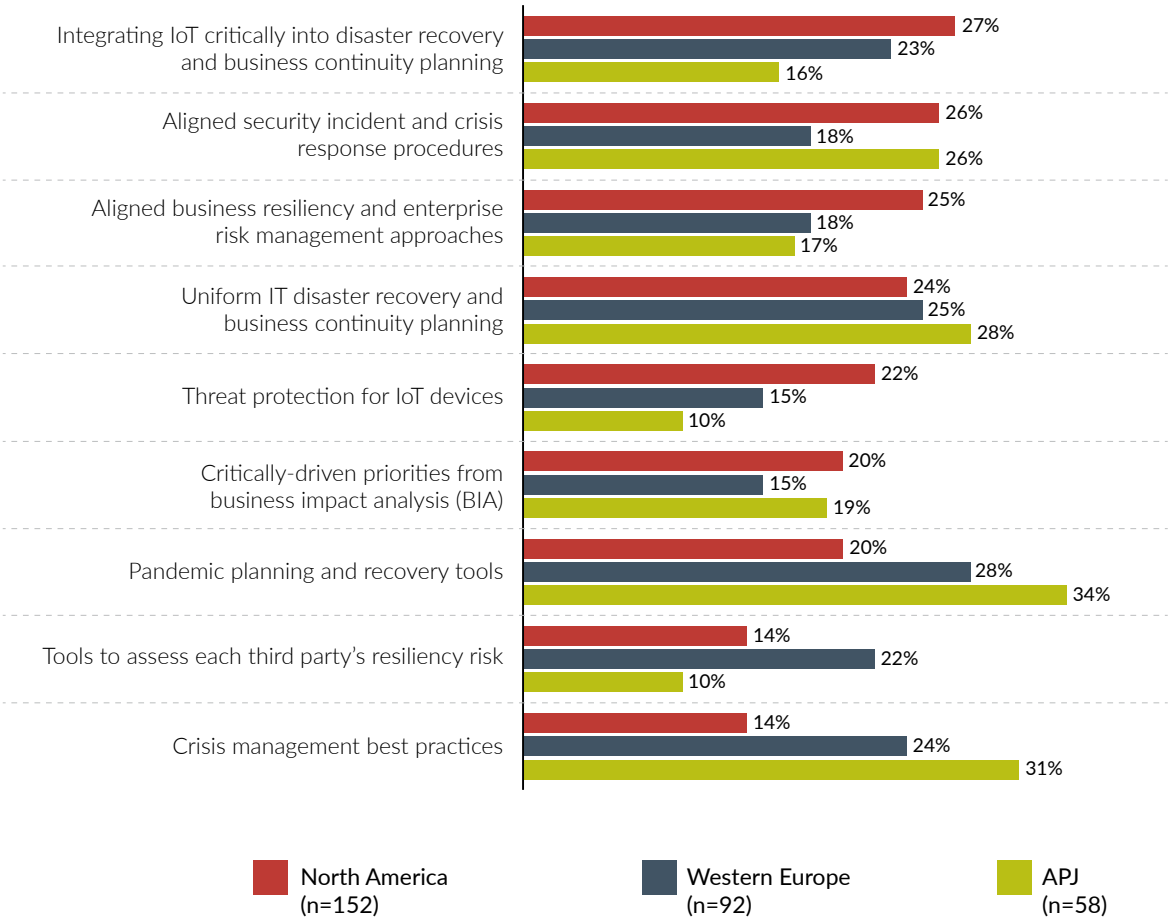
Focus on resiliency

Some respondents indicated that their organizations have been less successful in managing their risks during the pandemic, as shown in figure 10. We asked respondents from these organizations to indicate the specific area in which they've been most challenged. Ensuring business continuity, disaster recovery and crisis response emerged as the greatest challenges.

There are many technologies organizations can implement to manage business continuity, disaster recovery and crisis response risks. We asked respondents which of these types of technologies will be most important to their organizations over the next two years. Their answers, shown in figure 13, provide guidance on the technologies that organizations can adopt or extend to address business continuity risk management challenges within their region's risk environment.

These findings highlight for organizations the importance of managing IT disaster recovery and general business continuity from a single, cohesive platform.

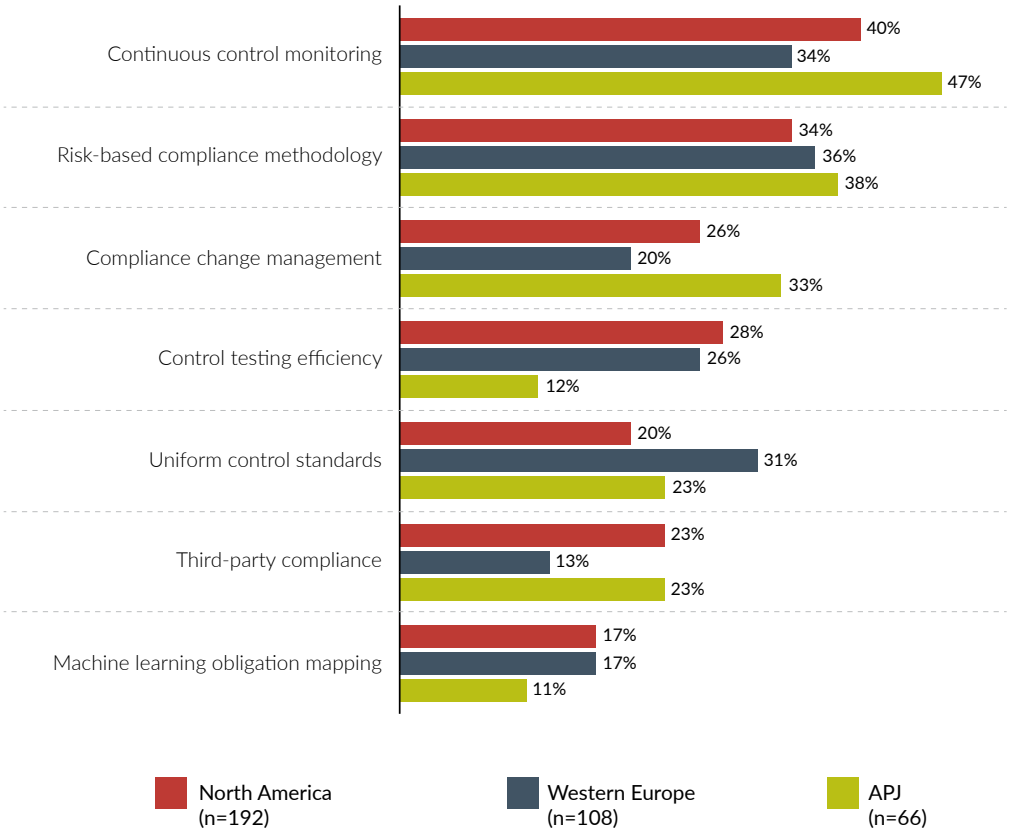
Figure 13. Planned Technologies to Address Business Continuity Risks



Adjust to compliance shifts

Compliance risk management was a top objective for many organizations, especially from respondents in Europe. To ensure compliance (including laws, regulations, policies, procedures, and contractual obligations) throughout their digital transformations, organizations should plan to adopt or extend continuous compliance controls monitoring and apply risk-based compliance methodologies, as shown in figure 14.

Figure 14. Planned Technologies to Address Compliance Risks



Recommended next steps

Advance planning and investments for managing risks associated with digital transformations is key for organizations to sustain their operations during major disruptions. Organizations must focus on the risk management technologies that will be most effective for the risk environment in their regions.

The survey findings suggest all organizations should adopt or expand multi-factor or passwordless authentication and risk-based authentication. Organizations in Western Europe should also focus on risk-based compliance methodologies and continuous compliance controls monitoring. Organizations in APJ will benefit especially from risk management solutions that integrate IT and general business disaster recovery in one platform, with pandemic planning tools included.

Integrating Risk and Operational Resiliency

A case for operational resiliency

Operational resiliency refers to an organization's ability to absorb and adapt to rapid changes, sudden disruptions or other challenges—and continue to achieve its objectives. Operational resiliency (or business resiliency) isn't only about business or IT recovery after a disruption; it also includes building resilient business practices across the organization to prepare for disruption. This is not just for the business continuity management (BCM) team—all parts of the organization must participate. For example, finance teams should ensure there are enough funds for executives to compensate for revenue declines or to allocate to growth opportunities. Procurement teams should ensure suppliers are diverse and redundant in case a key supplier is unable to keep pace or meet contractual requirements and service level agreements. Business teams should ensure the portfolio of customers isn't too heavily weighted toward a particular demographic, leaving the company exposed to revenue impacts if demand declines. IT teams should ensure that new systems are developed not only for efficiency but also for adaptability to changing business demands and digital transformation opportunities. In short, building resiliency is just good business practice.

Operational resiliency (or business resiliency) isn't only about business or IT recovery after a disruption; it also includes building resilient business practices across the organization to prepare for disruption.

Resilient organizations not only weather proverbial storms better, but also thrive in spite of them, as highlighted by a McKinsey & Company study[1] showing that after the 2007 financial crisis companies they characterize as "resilients" significantly outperformed "non-resilients" and the S&P 500 for several years post-recovery. What's more, global regulators, particularly in the financial services industry, have been placing more emphasis on resiliency since the financial crisis of 2008. We expect this trend to continue and extend beyond financial services to other industries that have been adversely impacted by the events of 2020.

How does an organization know if it's resilient? Many executive management teams are grappling with this question as they confront pressure from shareholders and regulators to ensure the ongoing viability and profitability of their businesses. Too often, the answer to this question only comes after a disruption has occurred.

Challenges to operational resiliency

Culture. One of the most difficult challenges in building operational resiliency is convincing the organization that it's not resilient enough, especially if a disruption has never occurred to expose a lack of readiness. Organizations may feel that their BCM program is enough, but BCM is usually focused on recovery versus building resiliency. Further, small BCM teams do much of the work of preparation and recovery, yet resiliency requires shared accountability throughout the business. Finally, although BCM gets executive attention during disruptions, once normalcy is restored the organization shifts back to business as usual, often leaving resiliency lacking. Whether it's due to organizational culture, inertia, or a lack of focus or resources, other priorities take precedence.

Complexity and maturity. The transition from only having a BCM (recovery) program to building operational resiliency is not easy. It's like going from freshman Introductory Chemistry 101 to senior-level Organic Chemistry 550. Traditional BCM is deployed in most organizations and is well-defined through a myriad of standards, methodologies and approaches. And although BCM is an important part of building resiliency, operational resiliency is much more than BCM—but it's also much less well-defined, and its implementation varies widely from one organization to another.

Organizational obstacles. Most organizations have siloed practices and information, particularly in the areas of operational risk management—IT risk, third-party risk, BCM, IT disaster recovery, crisis management and incident response. The issue is these teams aren't well-integrated. They usually have separate approaches, goals, teams and tools. To build operational resiliency, they must work much more closely together. Further, these teams tend to do most of the work because they're the experts. The business units, on the other hand, are less involved than they should be, resulting in a lack of buy-in, participation and accountability for operational resiliency.

Digital transformation. Digital transformation complicates efforts to build resiliency. It's not just the digital transformation and accompanying risks, it's also the speed at which companies are implementing digital transformation. The business may need to implement changes as quickly as possible, but the organization might not be ready to ingest and capitalize on them or determine how they impact the organization's resiliency.

Third-party ecosystems. Organizations rely on an ever-increasing and expansive ecosystem of third parties to broaden and optimize their capabilities. Yet responsibility for third-party resiliency rests upon the third parties, leaving the engaging organization with limited control. The growing number of third parties, the complexity of the relationships and the myriad of ways risk may arise from them increase the likelihood that the engaging organization's resiliency will be adversely impacted by these outside parties at some point. Also, the more critical the organization's dependence on a third party, the more likely any adverse impact could be catastrophic. As this ecosystem grows, it requires more risk-based governance because traditional methods are not scalable for growing third-party ecosystems.

Risk mismanagement. A final challenge to building operational resiliency is the lack of alignment between operational resiliency and integrated risk management, primarily due to the organizational and functional siloes mentioned earlier. Operational resiliency cannot be built effectively upon disparate risk management functions that use different approaches and have inconsistent priorities and separate silos of information. Also, risk functions that are divided between business risk and IT risk do not lend themselves to the holistic evaluation and mitigation of risks that could improve the resiliency of digitally transforming organizations.

These and other factors make building operational resiliency more difficult, but not impossible.

Operational resiliency cannot be built effectively upon disparate risk management functions that use different approaches and have inconsistent priorities and separate silos of information.

Overcoming challenges and building resiliency

Commit to organizational alignment. It truly "takes a village" to build operational resiliency. If an organization's goal is to become resilient, direction must come from the board and C-suite. Further, the resiliency function must report to a senior executive that can effect strategic change. And finally, leaders must commit to dedicating time and resources across the organization: BCM, business operations, IT, procurement, sales, integrated risk management teams and other functions.

It truly "takes a village" to build operational resiliency. If an organization's goal is to become resilient, direction must come from the board and C-suite.

Leverage digital transformation. Implementing new technologies can either enable organizational resiliency or complicate it. The RSA 2020 Digital Risk Survey asked respondents which technology deployed during the global health crisis was most helpful. Top answers included remote work infrastructure, security and fraud capabilities, and the cloud. However, a significant number also mentioned IoT, robotics or AI—all vital but not always friendly to building resiliency due to their complexity, new risks or operational nuances. Thus, as organizations continue to transform digitally, even during disruptions and downturns, they must do so in measured ways that enable them to successfully adapt and implement digital technology, adjust business processes accordingly, and mitigate any gaps in resiliency the new adjustments may cause.

Rely on integrated risk management. Integrated risk management plays an important part in building resiliency by helping to identify and mitigate resiliency risks. This is best accomplished when all risk teams follow a common process with similar goals—not just risk appetite, but resiliency goals and measures—and use an integrated risk management tool that provides common workflows, reporting and metrics.

Build third-party resiliency. The first step to managing resiliency of third parties is aligning their resiliency objectives with those of your own organization. Third parties must be thought of as a vital extension of the engaging organization and managed just as consistently. This starts in the contracting stage with identifying resiliency gaps and resolving them and lining up resiliency goals and metrics. It continues with assessing and monitoring the third party's resiliency throughout the life of the relationship. You also want to consider your entire ecosystem of third parties and the resiliency risks that ecosystem poses to your organization.

Start building resiliency now

The French aviator and writer, Antoine de Saint-Exupéry, said, "It's never too late to do something." One way is to start with an assessment of your organization's current resiliency posture that compares your current maturity level to your desired maturity level. This exercise will highlight the most important gaps and suggest where your organization should allocate resources. Building operational resiliency is a journey that must include the entire organization and, if there is constant emphasis and attention, one that will strengthen your organization and its ability to successfully achieve its objectives.

Survey Methodology

RSA commissioned independent research firm Vanson Bourne to execute the survey for the RSA Digital Risk Study 2020. 1,000 respondents completed the double-blind, online survey.

To participate in the survey, respondents were screened for the following qualifications:

- Working full-time in a supervisory or higher role
- Working for an organization that is engaged in digital transformation, or planning to execute a digital transformation initiative in the next two years
- Involved in (such as influencing or approving) their organization's digital transformation purchasing decisions

Guided by RSA, Vanson Bourne imposed quotas on the respondent pool to help ensure the results reflected a representative sample of organizations that are or may soon be implementing digital transformations. Quotas were based on:

- Respondents' departments
- Respondents' organization size
- Respondents' industry

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

1. Hirt, Laczkowski and Mysore, "**Bubbles Pop, Downturns Stop**," McKinsey Quarterly, May 21, 2019