

# In a world of risk, pace comes from preparation

Accenture 2021 Global Risk Management Study

# Contents

Executive summary	3
Yet more complexity	6
Technology and the risk function: Cutting through complexity	11
Hone the skills and focus of risk to transform	17
Prepare for the crisis just around the corner	21
Reposition risk to safeguard growth	25
Conclusion	30

# Better preparation leads to faster execution

In the weeks leading up to the 24 Hours of Le Mans (24 Heures du Mans®) sports car endurance race in 1953, few commentators looked past the established favorites for the potential winner. All had designed and built brand new cars for the race. And, more importantly, almost every motorsport world champion competing at the time was set to drive for these manufacturers.<sup>1</sup>

No one held out much hope for the small, UK-based manufacturer. The previous year, all three of its cars had retired early in the race owing to engine failure. Yet, against all expectations, their four participating cars finished first, second, fourth, and ninth—a remarkable achievement, given that 60 cars started the race. In addition, the winning car clocked a new record: for the first time, a car averaged more than 100 mph and completed more than 300 laps over the 24-hour period.<sup>2</sup>

What was the secret to this technology triumph? Key to its success was the use of disc brakes for the first time, which were much more reliable than its rivals' conventional drum brakes. Despite other cars' superior speeds in the straights, the UK race team's cars could hurtle into the track's many corners much more aggressively, knowing that their innovative brakes could slow them down. Rather than tweaking existing components of their car, they completely innovated a new solution. And combined with their advanced steering and rapid acceleration, the cars could complete the laps faster than their competitors.

Today, almost 70 years later, businesses and risk leaders, can learn much from this UK-based team, as well as from the efforts and preparation required across many disciplines. The meticulous planning needed to scale a mountain, the grueling training required over months to execute a perfect 100M sprint in seconds, and the innovation and insights required to cross an ominous ravine or barren desert all serve as appropriate metaphors for what is required of risk professionals today given the challenges they face.

In all these examples, it is fresh thinking, foresight and innovation – increasingly supported by technology – that allows individuals to identify and navigate threats earlier and more effectively. The same is required of risk professionals today. Business leaders who are effectively supported by risk teams in the same way can be ever more confident in their decisions – knowing that everything is being done to measure, manage and mitigate risks, allowing their business to transform at speed.



## Turning effort into outcomes

To understand how risk teams are progressing against a multitude of important areas, **we surveyed 725 risk leaders globally** from businesses spanning multiple sectors.

more than

**\$1B**

generated by every surveyed business

and more than

**\$5B**

generated by 54%

### Here's a snapshot of what we found:

- 77 percent of risk leaders believe that complex, interconnected risks are emerging at a more rapid pace than ever before. In parallel, operational and financial risks rose up the agenda most significantly in the past 12 months (see Section 1).
- Despite its growing importance, risk teams trail behind the rest of the business when it comes to deploying new technology: just 46 percent use cloud technology to process and derive value from data, which is less than teams in the wider business (57 percent) (see Section 2).
- Businesses have accelerated digital-transformation plans in response to COVID-19 and broader business challenges, but risk teams lack confidence in assessing risks associated with the technology that underpins them. Only 49 percent say they are “fully capable” of assessing risks associated with their businesses’ adoption of cloud. Even fewer believe they are fully capable of assessing the risks of artificial intelligence (AI) (34 percent), blockchain (32 percent) and robotic process automation (RPA) (28 percent) (see Section 3).
- Despite the health and economic challenges of the past 18 months, fewer than a third of risk leaders are “very satisfied” with their progress in bolstering operational resilience in the past two years. Furthermore, fewer than half took vital steps to fortify stress testing, such as expanding the range of scenarios covered or involving more stakeholders (see Section 4).
- Eight in ten risk leaders say their teams now spend significantly more time on value-adding activities such as product advisory or evaluating new business models, compared with two years ago. That said, the same proportion struggle to balance this with traditional duties such as reporting (see Section 5).

Whether it be the technology or data that is used by risk teams or the level of collaboration between risk teams and the wider business, a common theme emerges from the study data: risk teams have made incremental improvements and achieved pockets of success, but they are not making the progress required to manage the growing complexity of risk and the emergence of new threats. Some risk leaders may, in some cases, be satisfied with their progress, but the reality is that the gap is not being closed. Increased pace is required.

This has resulted in risk teams being reactive, scrambling to adjust when a major risk event materializes or when the business embarks on a new strategy with little warning. It has also heightened the potential for risk to lose credibility if it continues to lag behind the wider business. Without the right “intervention,” the lag is likely to get larger.

To accelerate pace, risk teams need to develop a robust platform from which they can scale and operate with agility. Innovation, preparation and then execution supported by data and insight remain as the ultimate objective. Practically speaking, this means adopting and using new technology effectively within the risk function; bringing new modeling, analytics and technology skills into the team; and forging deeper connections with the wider business, while maintaining independence to challenge business assumptions and practices. Across sectors, risk teams need to be better equipped and connected than they are today to manage the complex risk environment, and importantly to provide them with the credibility needed to support, challenge and help accelerate growth and transformation plans.



77%

of risk leaders believe that complex, interconnected new risks are emerging at a more rapid pace than ever before.

## Yet more complexity

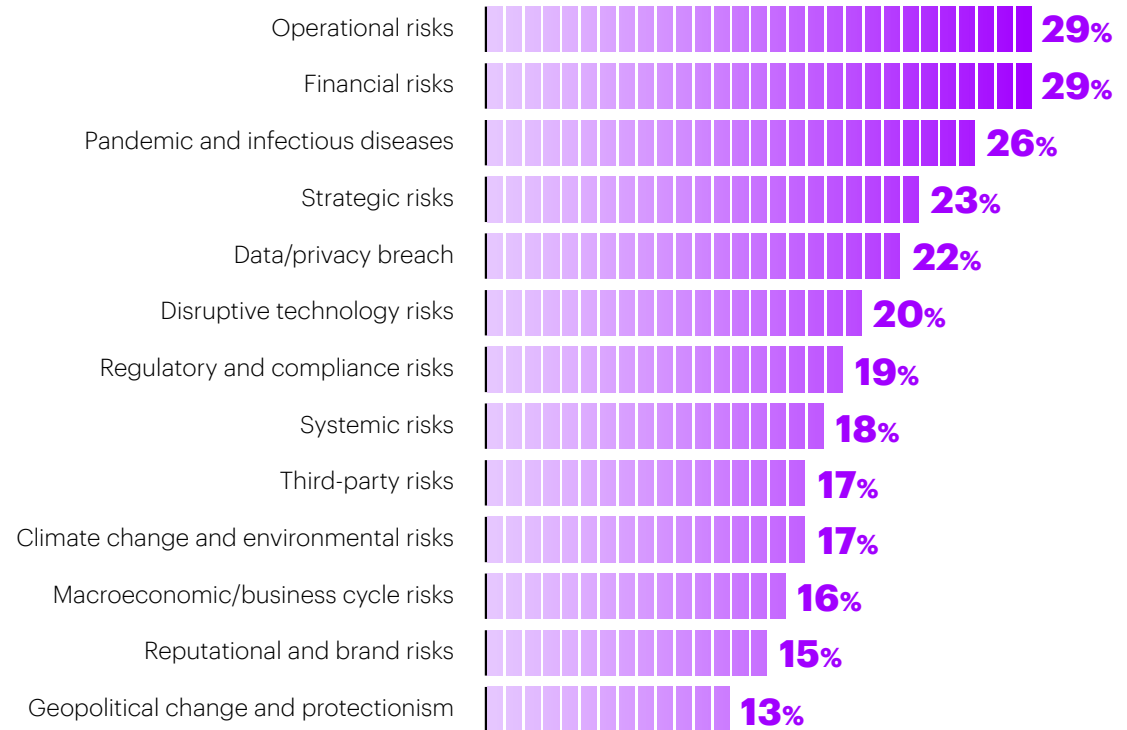
**Complex. Volatile. Fast-paced.** These are all words we used to describe the risk landscape two years ago when writing this report. These descriptions ring even more true today than they did then.

Whether it be supply-chain disruptions, impacts of cyber attacks, challenges of virtual working, or unstable market demand, the recent volatility has intensified and reshaped many risks that businesses face. Of course, technology disruption, climate change and geopolitical tension were already creating complex risks long before the pandemic arrived. And new sources of complexity continue to emerge every day. What new risks will the gradual return to the office entail? What new extreme weather events will climate change cause? And will consumers' expectations and behaviors, which changed so significantly at the height of COVID-19, switch again as the pandemic finally recedes?

It's no wonder 77 percent of risk leaders believe that complex, interconnected new risks are emerging at a more rapid pace than ever before. Just as Le Mans race car drivers have to contend with rapidly changing weather conditions and sudden hazards should another car crash or issues emerge within their vehicle, risk teams are encountering unforeseen threats with increasing frequency.

When asked which categories of risk have risen furthest up the agenda in the past two years (see Figure 1), risk leaders most frequently mention operational (a greater challenge for the software and platforms sector) and financial risk (a more important issue for the utilities and energy sectors). Operational risks were exacerbated owing to the supply-chain disruption and drastically increased need for remote working brought about by the pandemic. There has also been a surge in cyber attacks that have the potential to shut down vital business systems.<sup>3</sup> Financial risks were compounded by concerns over credit risk, caused by the economic uncertainty.

**Figure 1.**  
Operational and financial risks increased most in importance



Source: 2021 Global Risk Management Study, Accenture



Other risk categories frequently mentioned by risk leaders as having risen up the agenda are (unsurprisingly) pandemics and infectious diseases; strategic risks (which encompass a range of threats, from disruptive market entrants with new business models to the emergence of new, game-changing technologies such as crypto-currencies); data and privacy breaches; and risks associated with implementing disruptive technology.

Some sector-specific variations exist. For example, risk leaders in the energy sector say strategic risks rose up the agenda most in the past two years while utilities businesses rank regulatory and compliance risks significantly higher than those outside this sector.

The fact that risk teams are fighting on many fronts means it's vital to bolster their capabilities. But, when we ask risk leaders about the work they have done in the past two years in response to this growing

complexity, just 29 percent say they are "very satisfied" with their businesses' progress in proactively identifying and defining new risks. In parallel, only 31 percent are "very satisfied" with their progress in reinforcing operational resilience.

There's also ample opportunity for risk teams to work more closely with the business in order to shed their reputation as a back-office function. But just 30 percent are "very satisfied" with their progress in the past two years in re-engineering the operating model so that risk works more effectively with other functions.

There is clearly more work for risk teams to do. This includes a renewed focus on smart technology and data, enhancing skill sets, and repositioning the risk team so that it has a seat at the table during major business-transformation initiatives.

## Regulatory risk: Heightened complexity calls for a strategic approach

Whether it be with respect to business resiliency, climate change, or data privacy, new regulations continue to be written for which risk leaders need to be prepared to respond. In addition, regulators in certain jurisdictions are shifting to an “outcomes-based approach,” compelling businesses not only to comply with regulation to the letter but to deliver on the intended outcomes of the regulation—be those benefits to clients, the public, or other stakeholders.

This creates new complexity for risk teams and requires them to adopt a more strategic, connected approach, engaging closely with regulators and the wider business to make sure that the intent of regulation is understood and factored into business decisions.

Not surprisingly given the growing regulatory complexity, our study reveals that risk teams feel underprepared. For example, less than a third of risk leaders say they are “extremely confident” in their businesses’ ability to comply with new consumer privacy and data protection or operational resilience regulation. In addition, just 31 percent are “extremely confident” in their ability to communicate their business’s changing risk profile to regulators.

Of course, it is not solely the responsibility of risk teams to comply with new regulation, but there are many ways in which they can both lead and contribute. As a starting point, risk teams need to identify potential impacts of upcoming regulatory change in briefings and discussions, and through consultancy papers and regulatory presentations. They can also exchange insight into new and upcoming regulation by proactively engaging with regulators as to the impacts and feasibility of anticipated scope and timelines.

Beyond these manual approaches, risk leaders can deploy new technology to help their business understand and comply with regulation. For example, AI can be used to index, assess and disseminate new regulatory requirements to the wider business while analytics can be leveraged to unearth compliance bottlenecks. This type of “index of impacts” can help focus and prioritize remediation efforts that affect customer facing functions, pricing and other critical business activities.

One area where risk teams are sharpening their focus is climate-change regulation. For example, although just 49 percent currently evaluate climate-change-related regulation, a further 41 percent plan to do so.

In parallel, although just 41 percent incorporate climate change into scenario planning and stress testing, a further 46 percent intend to do so.

Risk teams in certain sectors are further ahead. For example, 50 percent of risk teams in the life sciences sector already factor climate change into scenario planning and stress testing, compared with just 28 percent in the utilities sector.





## Cyber risk: Amplified by remote working

Businesses have long contended with cyber threats, but the sheer number and sophistication of attacks ramped up in the past 18 months as malicious actors sought to take advantage of organizations' unusual working conditions. Illustrating this, Accenture's Cyber Investigations and Forensic Response team detected a 50 percent annual increase in business-email compromise events; a 160 percent increase in ransomware; and an almost 200 percent increase in third-party or supply-chain intrusions.<sup>4</sup>

Ongoing cyber-threat monitoring and detection is likely to fall outside the risk team's direct responsibility. That said, risk teams ought to evaluate whether the threat monitoring and vulnerability assessments undertaken by operational teams are sufficient, given the changeable nature of cyber threats.

In order to do this effectively, risk teams need to keep up to date with evolving threats. Notably, when

asked about their cybersecurity mitigation plans, risk leaders at large organizations (those generating \$5 billion—\$50 billion in annual revenue) say that improving their understanding of how cyber threats are exacerbated by remote working is their top priority.

The study data also reveals that risk teams in certain sectors prioritize different cybersecurity mitigation initiatives. For example, those in the telecommunications sector prioritize developing a risk-based approach to cybersecurity, whereby the business's most valuable assets are more robustly protected than those that are less valuable. By contrast, risk teams in the life sciences sector more often prioritize clarifying the delineation of responsibilities between the risk function and cybersecurity and IT teams. Regardless of the approach taken, cyber attacks are becoming more sophisticated, creating a greater need for advanced risk and control frameworks.

A person riding a bicycle on a dirt trail through a vast, layered, reddish-brown desert landscape. The terrain is characterized by numerous rounded, eroded hills and ridges, creating a complex and textured environment. The lighting is warm, suggesting a sunset or sunrise, which highlights the intricate patterns of the rock formations. The overall scene conveys a sense of adventure and navigating through a challenging, complex terrain.

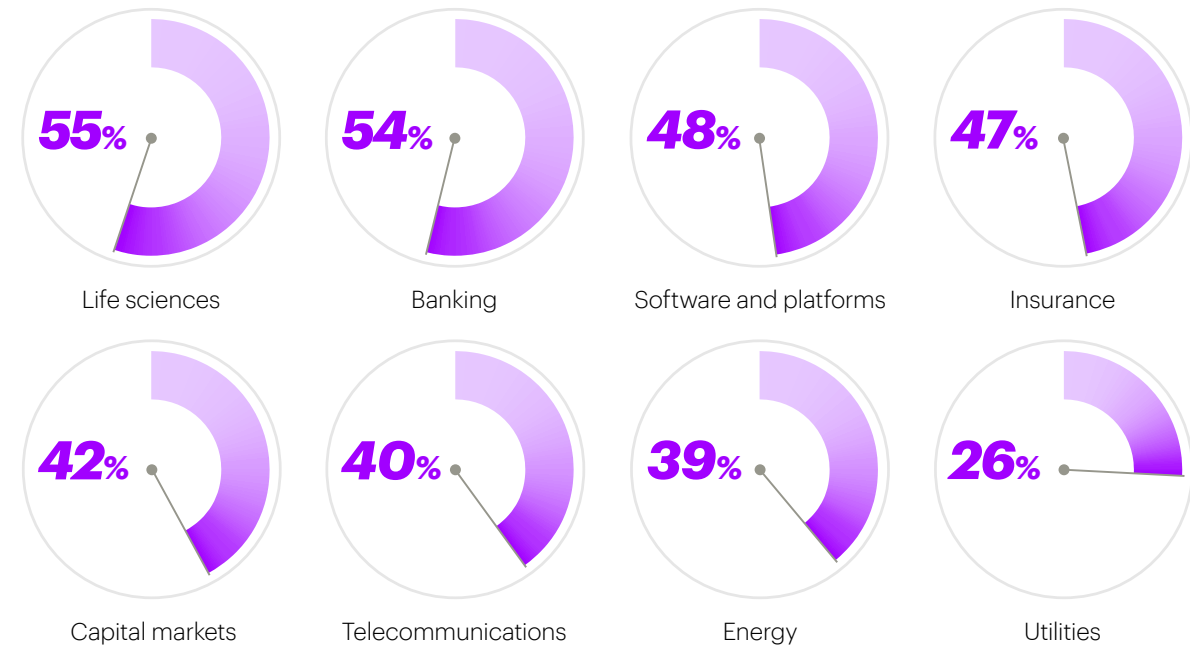
# Technology and the risk function: Cutting through complexity

## Being a fast follower in technology adoption is not an option

Surveyed risk leaders appear quite content with the steps they have taken recently to better utilize technology: 79 percent say they are satisfied with their progress in the last two years in implementing smart technologies to improve decision making in the risk function. However, technologies and related challenges are moving faster than the risk function, creating a widening gap in many important areas of need.

Our study data reveals that risk teams lag behind the wider business in terms of technology use. For example, although there are some sector differences (see Figure 2), 46 percent of risk teams use cloud technology to process and derive value from data, which is less than teams in the wider business (57 percent).

**Figure 2.**  
Risk teams at life sciences and banking businesses are furthest ahead in adopting cloud



Source: 2021 Global Risk Management Study, Accenture



Progress has no doubt been made, but the reality is that many risk teams are not where they ought to be in terms of technology adoption. Even those that have adopted technology such as cloud may be failing to take advantage of its full potential—for example to run more complex modeling or scenario planning.

Although slow uptake of technology could be excused in the past owing to limited budgets, siloed data, and other investment priorities, this is no longer the case. Just like our innovative Le Mans racing team took a giant stride in using new technology when it first used disc brakes almost 70 years ago, risk teams today need to take an equally bold and decisive step.

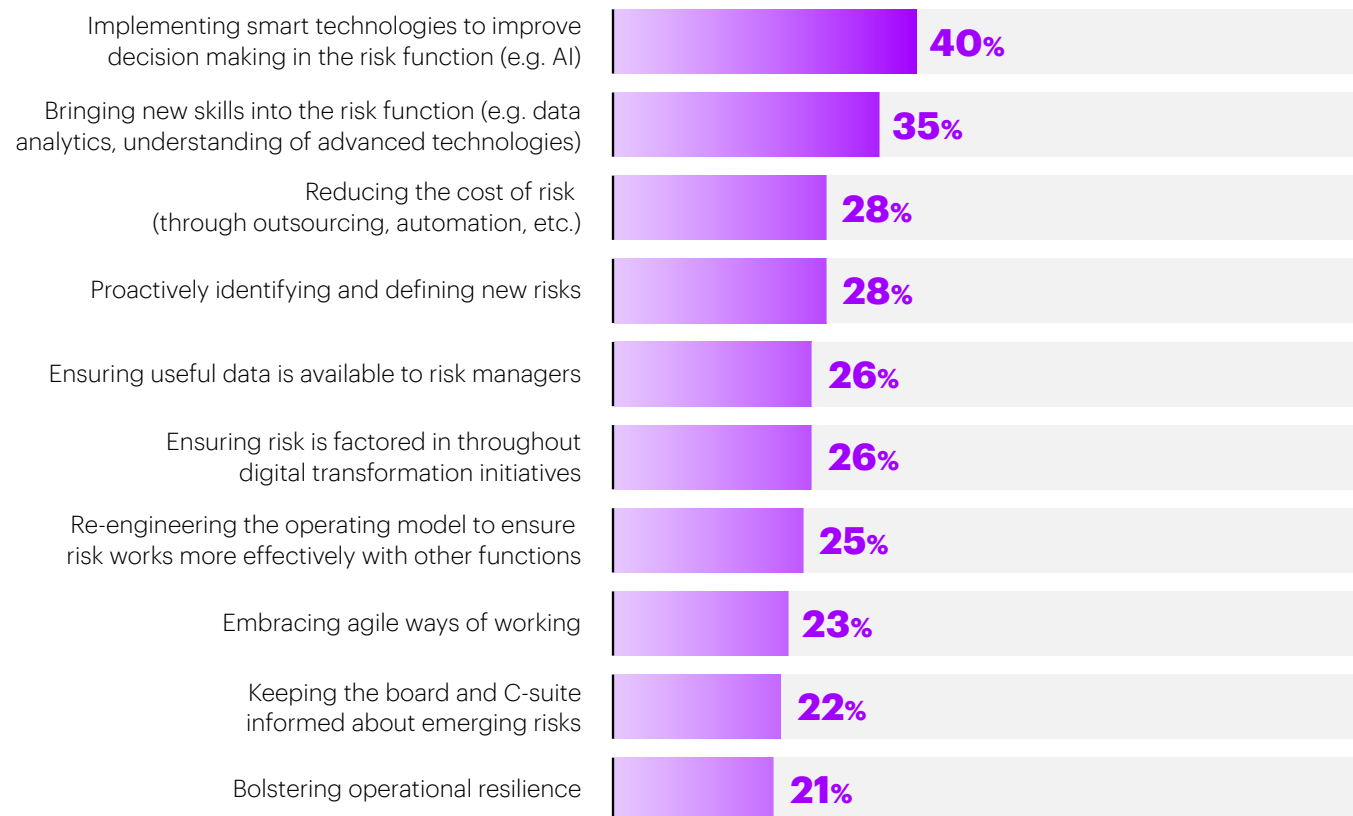
What does this mean in practice? Take, for example, the stress testing conducted by banks. To evaluate their exposure to mortgage defaults, many

banks previously relied on third-party economic data to augment their own data. Given the heightened volatility of the current financial climate, many today seek to incorporate consumers' employment status, sector, address, and other factors. This more sophisticated modeling requires the data-storage and analytics firepower that a cloud infrastructure is designed to deliver.

Stress testing aside, a combination of AI, RPA, and other technologies can also be deployed to automate basic processes, such as controls testing and reporting. This not only reduces cost but improves accuracy and frees up risk professionals' time for more strategic activities. It is this combination of human and machine that allows risk teams to effectively oversee risk. Without it, they not only lose their ability to manage traditional risks, but also fail to create the capacity to evaluate new and emerging threats.

Risk leaders acknowledge this urgency: they identify implementing new tech as their top priority in order to cope with added complexity (see Figure 3). But there are opportunities to take this further: they should also make the business case for the front line of the organization to digitalize and automate processes—such as Know Your Client (KYC) checks—in such a way that it makes it easier to monitor and report on risks.

**Figure 3.**  
**Implementing smart technologies is the top priority of risk teams**



Source: 2021 Global Risk Management Study, Accenture

## Don't overlook technology skills

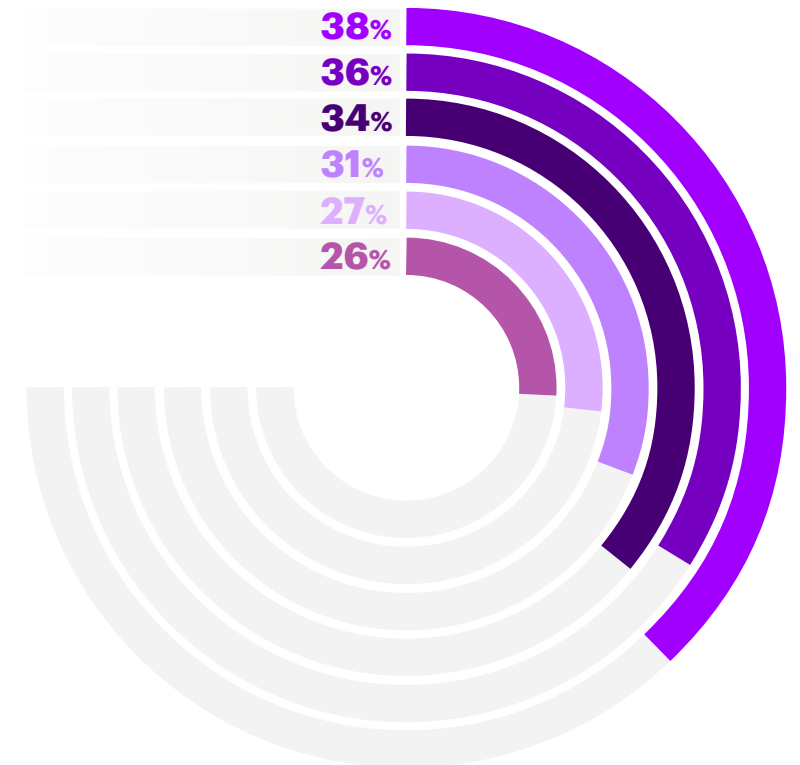
Historically, a lack of technology knowledge held risk teams back from implementing smart technology. Although technology evolves more quickly than executives and risk teams can embrace and deploy it, risk leaders need to strive to continually sharpen their technology capabilities.

Encouragingly, 35 percent of risk leaders identify bringing in new skills to the risk team as a top-three priority, making it the second-most-frequently selected priority area. But, when asked which capabilities they are prioritizing for improvement, skills associated with assessing and or applying disruptive technologies only ranked fifth (see Figure 4).

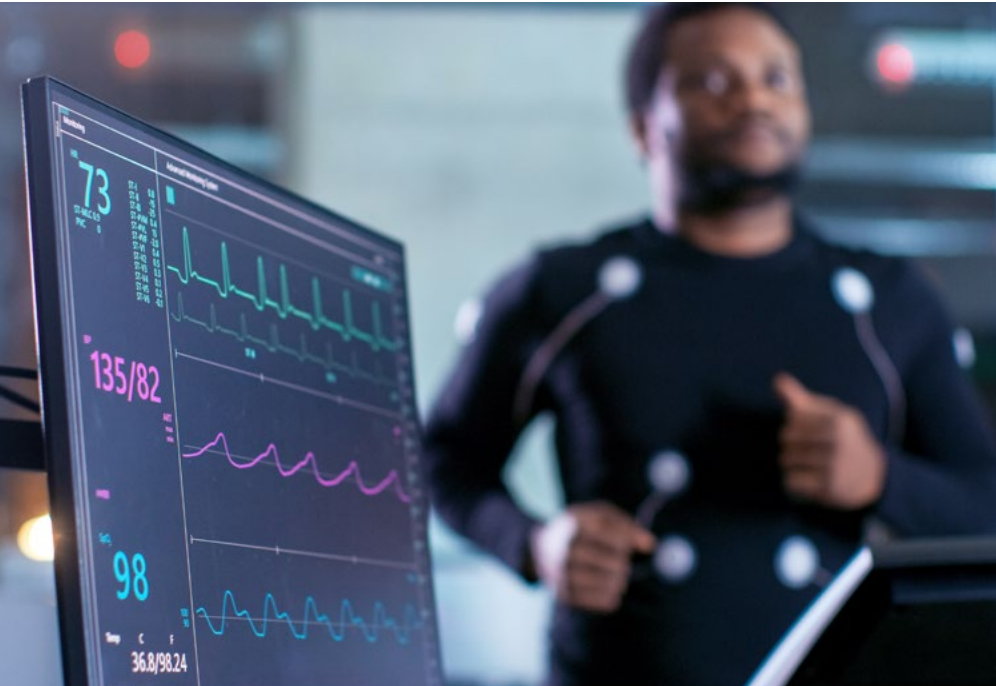
So, although it's encouraging that bringing skills into the risk team is high on the agenda, the comparatively low level of importance attached to recruiting those capable of assessing and applying disruptive technologies needs to also be addressed. When doing so, risk leaders need to evaluate how to rapidly address this skill set and to keep it current through a mix of recruiting new skills into the function and also tapping into the experience and knowledge of third-party providers to narrow gaps within the team. This type of skills expansion and balancing is expected to continue in the foreseeable future as businesses progress on their digital growth and cloud agendas.

**Figure 4.**  
Improving advanced data- and analytics-modeling capabilities is a top priority

- Advanced data analytics and modeling
- An ability to identify changes in the external risk environment
- An ability to drive collaboration with other functions while maintaining effective independence and challenge
- A deep understanding of industry/market trends
- Assessing and/or applying disruptive technologies
- General GRC (governance, risk and compliance) capabilities



Source: 2021 Global Risk Management Study, Accenture



## The data imperative: Turning intent into success

The study data also reveals that many businesses are progressing and improving the use and quality of data for better risk analysis: eight in ten are urgently improving their ability to collect and analyze enterprise-wide data. The same proportion is seeking to improve their ability to understand how risks are connected through integrating data sets.

This is a positive outcome, especially as the majority of risk leaders alongside their business counterparts have spent huge sums in recent years attempting to improve their data organization—often improving but not fully resolving the challenges they face.

So, how can they make more than incremental improvements? One further step risk teams can take is to work in a more closely connected manner with the data-support team across the business. In addition, risk leaders should explore the benefits of investing in the increasingly sophisticated big-data and AI-based tools that help businesses to aggregate, synthesize, and generally manage their data.

There is also a tremendous opportunity to hone risk modeling by combining internal and external data in order to better understand changing risks. For banks, for example, this has become imperative because traditional credit signals have been muted owing to COVID-19 stimulus. As a consequence, some banks are combining their own data with online reviews, for example, when assessing credit risk of hospitality businesses. Other banks have formed data-sharing partnerships with telecommunications businesses to understand better how consumers react to certain events. For other businesses, it may make sense to get even more insight into risk by incorporating environmental, social, and governance (ESG) data into their analyses.

# Hone the skills and focus of risk to transform



## Risk teams need to be closely connected to effectively deliver digital transformation

Whether it's the rollout of cloud, AI, RPA, or other new technologies, businesses' digital-transformation plans have accelerated in response to the pandemic and broader business challenges. Just look at cloud adoption: research shows that 90 percent of businesses expect cloud usage to exceed previous projections, in part, owing to COVID-19.<sup>5</sup>

While digital transformation plans bring tremendous opportunities—Accenture analysis reveals that increased use of technology to drive efficiency, insights, and capabilities results in significant profit benefits<sup>6</sup>—it can also carry certain risks. These include new cyber vulnerabilities, elevated potential for financial crime, unintended consequences of AI, and data-transformation issues. So, just as Le Mans racing teams need to understand the potentially detrimental knock-on effects of fitting new components to their vehicles, risk teams need to understand the risks associated with their business's use of new technology.

To make sure these threats are mitigated effectively, risk teams need to work with IT and other stakeholders to create a framework

to effectively manage the broad set of risks associated with large-scale technology implementation. In parallel, they have to insert themselves early in any transformation initiative to make sure that risks across the multiple impacted dimensions are being considered. In addition to making sound business sense, organizations in heavily regulated sectors have certain operational-resiliency requirements relating to technology change, which also necessitate a stronger risk-based view of digital transformation.

But strong participation from risk teams won't just mitigate the downsides of technology transformation; it can also speed up the business transformation itself. For example, onboarding a new cloud vendor could take up to six months once compliance, data, procurement, and other

teams have conducted due diligence. By implementing a risk-control framework, risk teams can complete onboarding more swiftly and effectively.

Risk teams can also deploy the risk modeling (such as Monte Carlo simulations) that they routinely use to simulate traditional risks to model and predict delays to major technology implementations and help identify issues in advance.

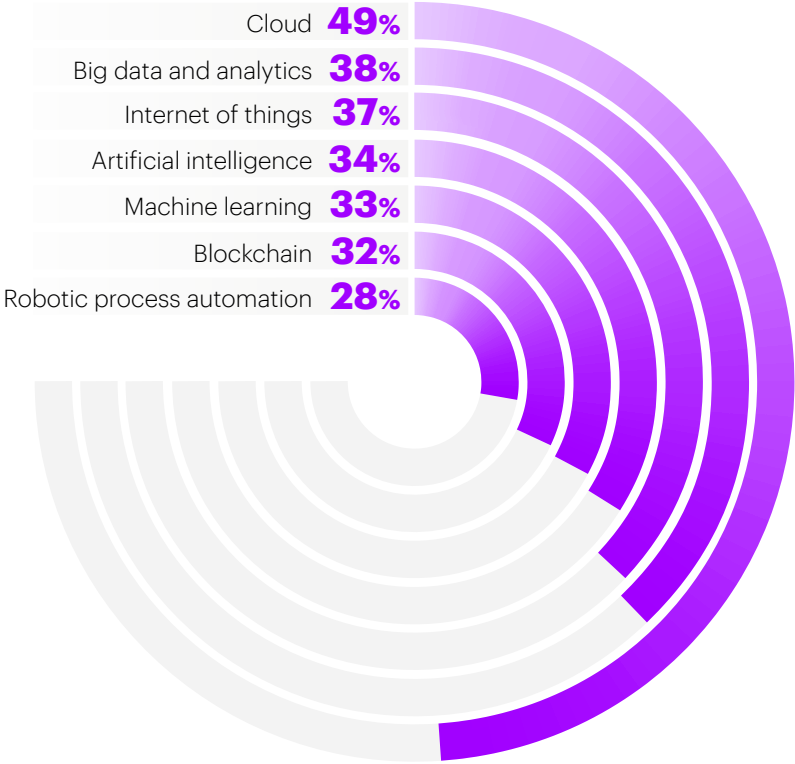
**Bottom-line, in order to keep up with the increasing pace of business change, risk functions need to reassess all of their foundational capabilities in order to accelerate.**

## Position risk to overcome digital-transformation roadblocks

Despite the growing necessity for risk teams to participate in major digital-transformation projects, the study data indicates that less than a third are “very satisfied” with their progress in doing so over the past two years.

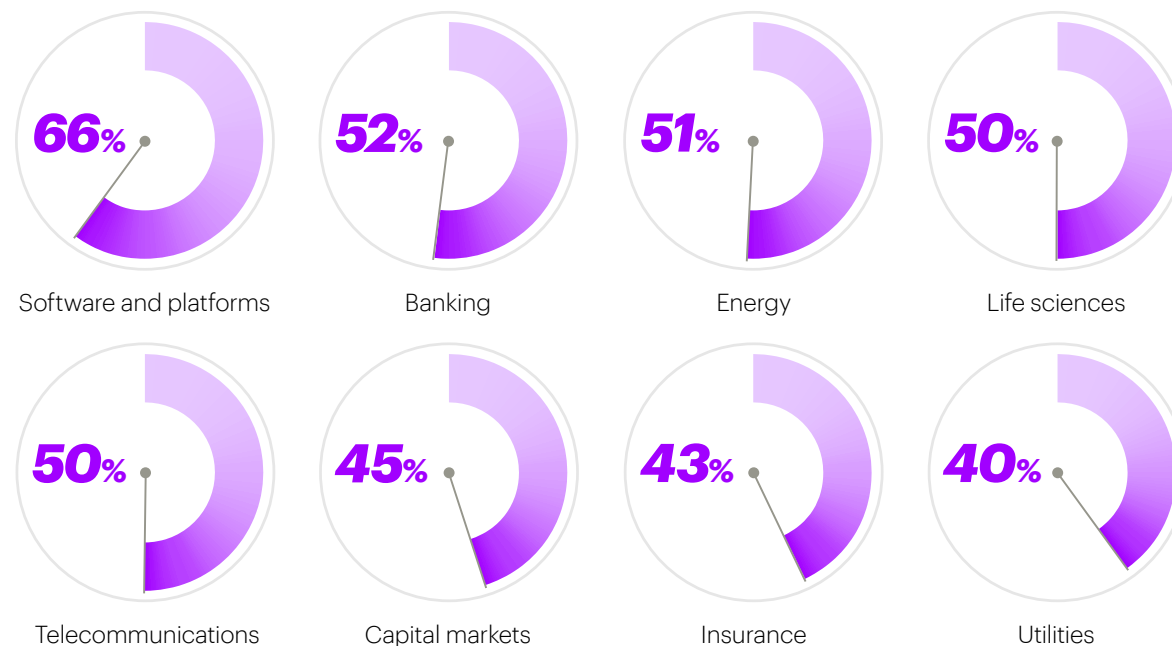
Moreover, the study data indicates that risk teams do not believe they are fully capable of assessing risks associated with the adoption of more advanced technologies. Only 49 percent believe their teams are “fully capable” of assessing risks associated with their business’s adoption of cloud. Fewer believe they are fully capable of assessing risks associated with their business’s adoption of AI, blockchain, and RPA (see Figure 5). There are some notable differences across sectors, with significantly more risk teams in the software and platforms sector being fully capable of assessing risks associated with cloud adoption than those in the capital markets, insurance or utilities sectors (see Figure 6).

**Figure 5.**  
Fewer than half of risk teams are “fully capable” of assessing new technology risks



Source: 2021 Global Risk Management Study, Accenture

**Figure 6.**  
**Risk teams in the software and platforms sector are most confident in assessing risks associated with cloud adoption**



% that consider their risk team 'fully capable' of assessing risks of adopting cloud  
 Source: 2021 Global Risk Management Study, Accenture

So, how can risk teams better equip themselves to manage these threats? As a starting point, they should think more creatively about the risks that could arise from major technology transformations. For example, the risks associated with the rollout of AI include bias and privacy threats that risk teams may not be used to monitoring. They should, therefore, sharpen their existing capabilities, such as model-risk management, to address them. Furthermore, if risk leaders and the risk function are not actively making use of these technologies, it is difficult for them to be seen as credible and insightful in evaluating risks in other areas of the business.

In addition, risk teams should review how they are organized to take advantage of the new ways of working in a more agile, digital-enabled world. For example, onboarding a cloud vendor requires operational, fraud, credit, regulatory, and various other types of risk to be assessed. Rather than structuring risk teams around categories of risk, it may make more sense to create a dedicated team within the risk function that works on onboarding cloud vendors. As this team works on more cloud implementations, they would naturally build their confidence and knowledge in assessing the potential risks specific to this category.

Even if such a team exists, its effectiveness would be minimal if it is siloed within the risk function. Instead, the operating model of the risk team should be such that it is in close proximity to the business and the digital transformation initiatives that it is undertaking.

# Prepare for the crisis just around the corner



Just

31%

of risk leaders are “very satisfied” with their progress in bolstering operational resilience in the past two years.

## Constantly prepare for the future... or jeopardize what you’ve built in the past

In light of the disruption and ongoing volatility, organizations need to build financial and operational resiliency against an increasingly unpredictable array of shocks and risks. In addition, new regulation requires businesses to adopt a much more robust approach to resiliency.

Despite its growing importance, just 31 percent of risk leaders are “very satisfied” with their progress in bolstering operational resilience in the past two years. Moreover, when asked about their current priorities, risk leaders rank fortifying operational resilience last.

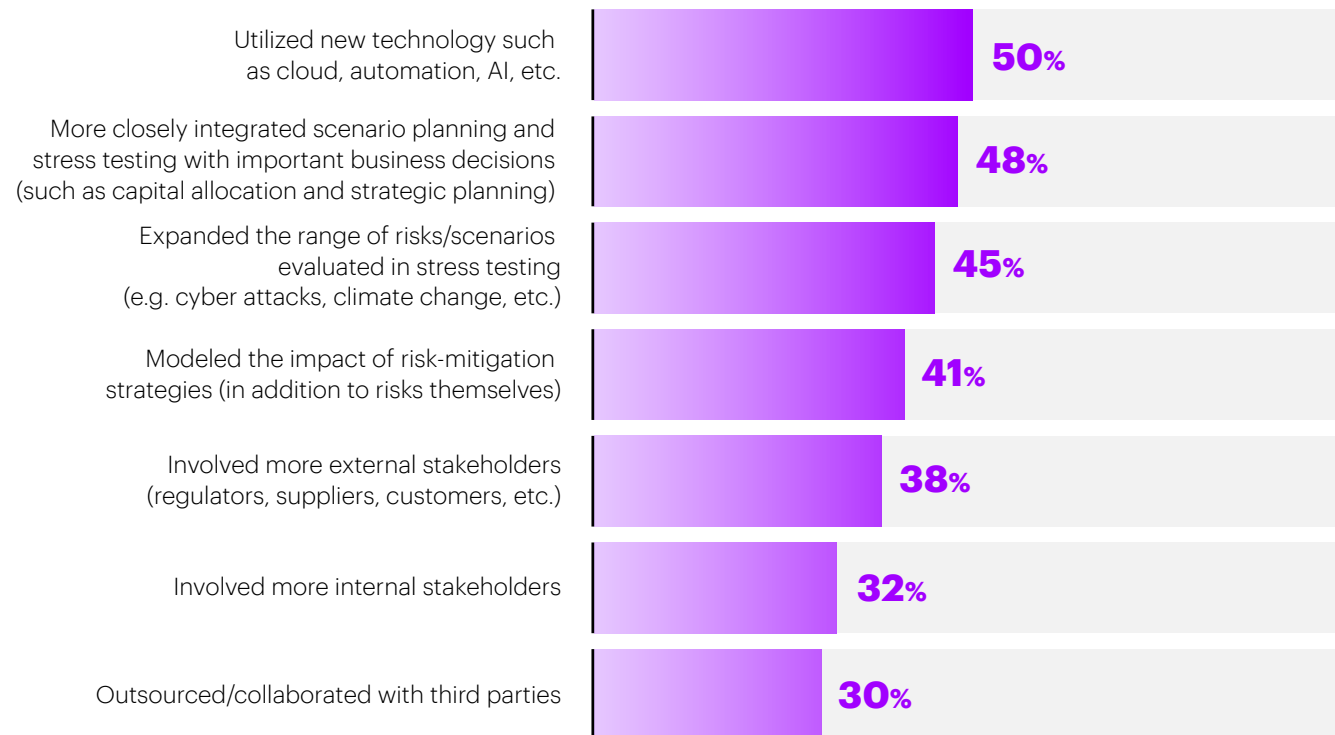
Nevertheless, preparation is absolutely vital. Just as Le Mans competitors begin to prepare for the one-day race as soon as the prior year’s race concludes, risk teams need to build up business resiliency to potential crisis events continually. In short, endurance isn’t about one day: it’s about every day.

What practical steps can risk teams take to strengthen resiliency? Although the front line of the business is ultimately responsible for operational-resiliency testing, risk teams should provide independent scrutiny of the frequency and robustness of these tests. They should also make sure that the business tests its resilience against a broad set of severe but plausible scenarios.

As in other areas, our study data indicates that there is still much work to do here: just 45 percent expanded the range of risks and scenarios evaluated in stress testing in the past 12 months, and fewer than 40 percent involved more external or internal stakeholders (see Figure 7).

What’s holding risk teams back? Some may need to improve their operational and technology knowledge to enhance their ability to provide effective check-and-challenge mechanisms around operational-resiliency testing. For others, it may make sense to encourage the business to create a chief resiliency officer role to lead up this area.

**Figure 7.**  
**Businesses have not taken vital steps to improve crisis management**



Source: 2021 Global Risk Management Study, Accenture

## Scrutinize crisis-management plans

Even if businesses do everything possible to bolster operational resiliency, “disaster” inevitably strikes. When it does, businesses need to have in place robust, flexible crisis-management plans that can guide their responses. Just as racing car pit crews spend days strategizing and practicing how to respond should their vehicle falter, across sectors businesses need to devote the time to making sure that their crisis management plans are complete, well-communicated, understood and practiced.

The study data indicates that risk leaders are confident in their updated crisis-management plans: although 71 percent of risk leaders say that COVID-19 exposed deficiencies in their ability to respond to crises, 83 percent have updated their business-continuity plan in the past 12 months and 82 percent say their business-continuity plan is fit for purpose.

What practical steps can risk teams take so that their crisis management plans and

the strategy for executing them are fit for purpose? As a starting point, risk teams need to make sure that these plans contain all of the detail that is necessary, including prescriptive guidance that is practical and executable about how to respond to an adverse shock. In addition, they need to broaden the spectrum of potential shocks they cover. It’s not enough to create resilience to financial risks; preparation needs to also cover cyber attacks, supply-chain disruption, another pandemic, and other unpredictable events. Risk teams also ought to make sure the crisis-management plans are understood by those who have to use them and test the business’s ability to follow the guidance they contain in an adverse event.

To understand the latest industry thinking, and to avoid the inadequate crisis response that can create systemic risks, there’s great value in sharing crisis-planning best practice with industry peers, creating a self-supporting network that can withstand future shocks.





# Reposition risk to safeguard growth

Just as our UK race team’s powerful brakes allowed its cars to approach corners at higher speed, a strong and independent view from risk gives businesses more confidence in their growth and transformation plans and allows them to be executed at greater pace.

Encouragingly, the study data reveals that risk teams are increasingly participating in growth initiatives:

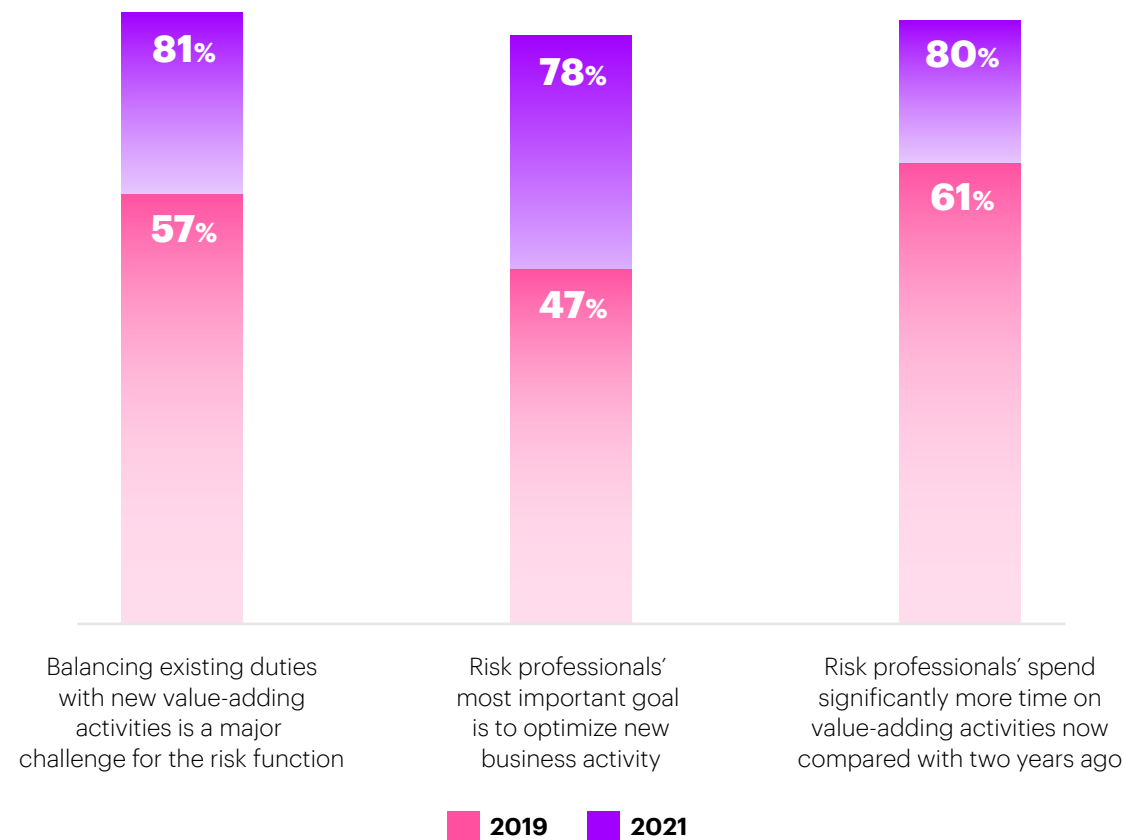
**80%**

of risk leaders say their teams spend significantly more time on value-adding activities now compared with two years ago

See figure 8

**Figure 8.**

Risk teams spend more time on value-adding tasks, but struggle to balance these with traditional duties



Source: 2021 Global Risk Management Study, Accenture



81%

say that balancing existing duties with value-adding activities is a major challenge

Although it's encouraging that risk teams increasingly participate in growth initiatives, the bad news is that 81 percent say that balancing existing duties with value-adding activities is a major challenge. Risk cannot engage in every growth initiative; instead, it needs to focus on those that are most critical to the viability of the business. And risk then needs to make sure that it has both the time and skills required in order to give these projects the attention they deserve.

But how exactly should risk teams participate in business-wide growth and transformation plans? Ultimately, their most important role is to make sure the "view of risk" is heard when their business evaluates transformation plans, major transactions, expansion into new markets, significant investments in technology, and other critical initiatives. Importantly, risk has to retain its role as being an independent and credible challenger, rather than just another voice in the room.

## Credibility through action

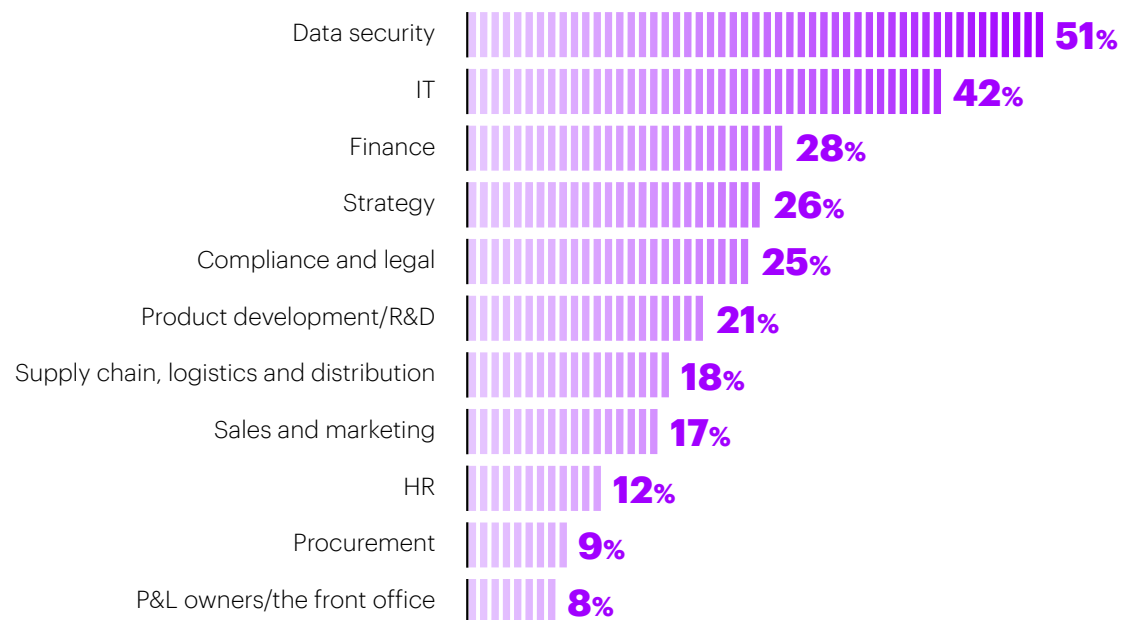
Risk management is about action; it is not a passive function. And for risk to influence the business to take appropriate action they need to be deemed credible by the business leaders they are engaging with. For example, risk teams within a bank can struggle to influence a strategy to expand lending into a new sector if it takes them weeks to develop models to evaluate credit risk in that particular industry. In addition, concerns that the risk team within a utility business might have about a cloud-migration strategy can carry much more weight if the risk team itself utilizes cloud extensively.

Perhaps even more importantly, the risk team also needs to bring qualified data to the table to back up its opinion about risks that may materialize from growth initiatives. Of course, this data needs to be translated into comprehensible, actionable insights for the wider business.

A good internal test of whether the wider business deems the risk team credible is whether it can articulate how risk is making a positive impact to their area of the business. Unfortunately, the answer is all too often 'no.' Risk needs to do a better job of articulating the positive benefit of their inclusion and demonstrate their valued impact. Without this understanding, there's a threat that risk teams may find themselves back in the pre-financial-crisis days, where they struggled to establish a seat at the table and materially influence business decisions.



**Figure 9.**  
Risk teams prioritize collaboration with data-security team



Source: 2021 Global Risk Management Study, Accenture

## Proximity to the business is key

Credibility aside, risk needs to have a close working relationship with the front office and teams that are leading transformation projects to exert its influence. However, the study data reveals that risk leaders instead prioritize fostering collaborative-working relationships with data-security and IT teams (see Figure 9). Furthermore, they rank profit and loss (P&L) owners and the front office as the last part of the businesses with which they need to foster closer ties.

In order to influence growth and transformation plans, risk teams first need to acknowledge the importance of being connected with and understood by the front line of the business. Then, they need to build these relationships. One practical way to do this is to rotate individuals between business and risk teams, allowing them to better understand each other's perspectives.

But there's an important balance to strike. Risk teams need to have a strong working relationship with the wider business, but not lose their ability to provide objective challenge and oversight.

# Conclusion: Going the distance

Whether it be their use of technology, their understanding of new threats or their participation in growth initiatives, risk teams undoubtedly made progress in the past two years. But the view from risk leaders themselves that is repeatedly conveyed in our study data is that this is not enough, especially given the increased complexity of risk.

This report outlines some further steps that risk leaders can take. Unfortunately, there are no quick fixes or silver bullets. Instead, just like Le Mans, this is an endurance race. Resilience comes from going the extra mile every day. This means experimenting with new technology, bringing new skills into the risk team, improving understanding of new digital threats and making sure risk is well connected with the rest of the business without compromising its ability to provide independent challenge.

The reward? Put simply, risk teams can improve their credibility and in turn, their influence. And with this, they are better positioned to mitigate new and emerging threats and give their business more confidence in growth and transformation initiatives.

**Ready. Steady. Go.**

## About the research

The Accenture 2021 Global Risk Management Study is the seventh edition of our study first published in 2009. It is based on a telephone survey (computer-assisted telephone interviewing, CATI) of 725 senior risk management executives conducted by Longitude, a Financial Times company, on behalf of Accenture between March 2021 and April 2021.

Survey participants were sourced from around the world and work in eight sectors: banking (181 participants); capital markets (153 participants); energy (70 participants); insurance (91 participants); life sciences (80 participants); software and platforms (50 participants); telecommunications (50 participants); and utilities (50 participants).

## About the author



### **Steve Culp**

*Steve Culp is a Senior Managing Director – CFO & Enterprise Value and responsible for our digital risk and compliance business globally. Based in Austin, Texas, Steve has 30 years of experience building our teams and capabilities in this space while working with clients across multiple geographies to define strategy and execute change programs across risk management and the broader finance function. His current focus is to work with client leadership to help them advance their business performance through innovative strategies, processes and change. Steve holds a Bachelor of Science in Finance and Economics from Northern Illinois University and earned an Executive Master of Business Administration degree at Kellogg in 1999.*

## Acknowledgments

We would like to thank the following Accenture leaders from North America, Europe and Asia Pacific for their contributions to this report:

**Chris Johnston, Eva Maybud, Michael McGinn, David Northen, Christian Pedersen, San Retna, Ben Shorten, Kuangyi Wei**

## About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. With 569,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at [www.accenture.com](http://www.accenture.com)

## References

- 1 Le Mans 1953: Jaguar’s gigantic leap, MotorSport, October 2020
- 2 1953 24 Hours of Le Mans: Night of the Disc Brakes, Jalopnik, August 2010
- 3 Looking back to see the future: CIFR DeLorean – 2021 edition, Accenture, February 2021
- 4 Looking back to see the future: CIFR DeLorean – 2021 edition, Accenture, February 2021
- 5 Cloud Computing Trends: 2021 State of the Cloud, Flexera, March 2021
- 6 Fast-track to future-ready, Accenture, January 2021

## Stay Connected

CFO & Enterprise Value:

[www.accenture.com/us-en/services/cfo-and-enterprise-value-index](http://www.accenture.com/us-en/services/cfo-and-enterprise-value-index)

Accenture Business Function – Finance blog:

[www.accenture.com/us-en/blogs/business-functions-blog/finance-index](http://www.accenture.com/us-en/blogs/business-functions-blog/finance-index)

Copyright © 2021 Accenture.  
All rights reserved.

Accenture and its logo are  
registered trademarks of Accenture.

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.