

2018 Risk in Review Study

Managing risks and enabling growth in the age of innovation



How can risk executives embrace innovation while preparing for unknown risks such as a self-driving car commandeered by hackers, data analytics software that unintentionally reflects biases, or autonomous weapons that cause accidental casualties? PwC explores how risk leaders can effectively manage innovation-related risk and by doing so, drive growth and performance. Key actions include linking an organization's risk program to corporate strategy and periodically adjusting risk appetite and tolerances to align with innovation risk.

Table of contents

Introduction	3
The state of innovation and the changing risk landscape	5
Effective risk management programs: Key attributes	8
Actions of effective risk management programs: Identifying, assessing, and adjusting for risk differently	12
The way forward: Obstacles to clear	22
Fueling growth in the age of innovation	25
Five actions to take today	26

Introduction

The present is marked by such change and innovation that it is described in revolutionary terms: *the fourth industrial revolution, the second machine age, the cognitive age*. And history teaches us that when innovation rises, so do risks. Kimberly Johnson, chief operating officer at Fannie Mae, recently captured that challenge well: “Innovation risk is a strategic question. The risk of not innovating is just as high as the risk of innovating, if not higher.”

As organizations increasingly face pressure to innovate, risk executives need to help their organizations strike the right risk–reward balance to succeed. After all, organizations that effectively manage innovation risk are more-effective innovators. But how should risk management programs evolve?

PwC set out to study that question in our *2018 Risk in Review Study*. How are risk management practices addressing innovation-related risk? How are they changing? Is risk management keeping pace, and if not, why not?

In late 2017, PwC polled more than 1,500 senior risk executives ranging from chief risk officers to audit/risk committee members, to CEOs at organizations headquartered in 76 countries about how they address innovation risk.

We also conducted in-depth interviews with eleven risk leaders. We found that 15% of respondents consider their risk management programs to be *very effective* in managing innovation-related risks. Another 45% consider their programs to be *somewhat effective*. We named these two groups collectively the Adapters with the defining tenet of this cohort adaptability.

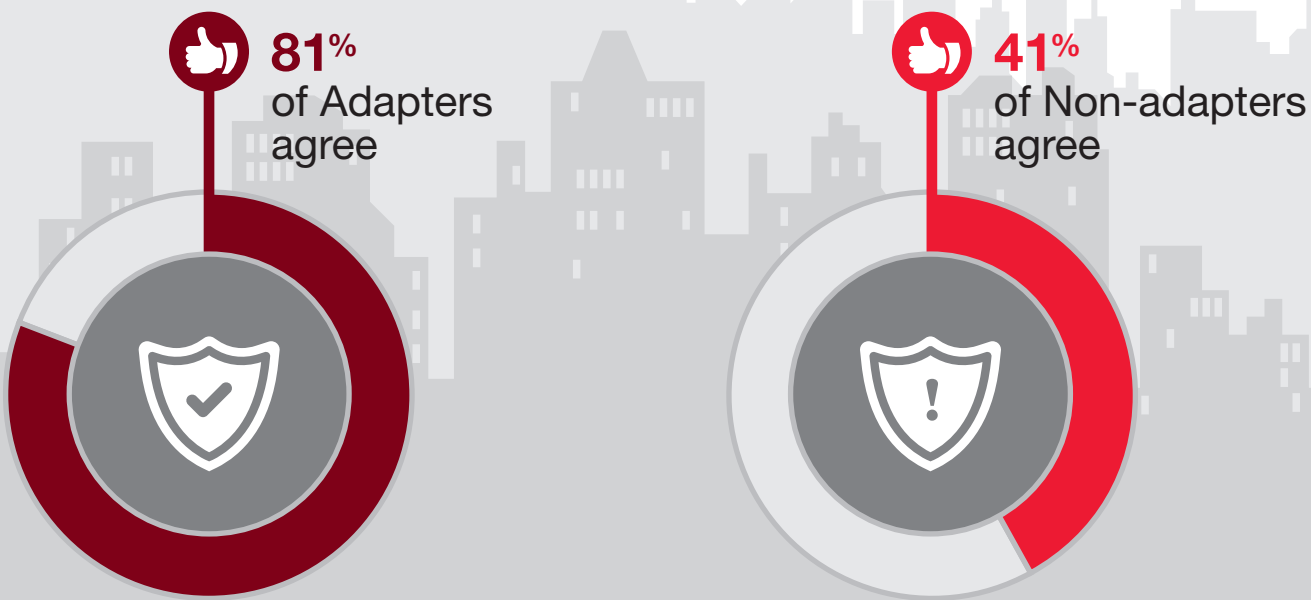
Adapters have already changed how they tackle innovation risk, but their practices differ in four key ways:

- The high level of involvement they have throughout the innovation cycle
- The multiple strategies they use to manage their exposure to innovation-related risk, led by sharing risk and adjusting the risk appetite
- The new skills, technologies, and capabilities they continuously add as they lean into innovation
- The broad set of mechanisms and metrics they use to monitor and measure their risk management programs’ effectiveness, to adjust for vulnerabilities as needed.

To keep pace with innovation and risks changing at breakneck speed, Adapters are harnessing a range of methods that will continue to grow and evolve along with these forces.

Risk executives who call their organizations more innovative than those of their peers and who consider their risk management programs to be more effective are three times more likely than their less-effective and less-innovative peers to anticipate revenue growth.

Figure 1: The risk management functions helps increase the odds of success



Source: PwC, *2018 Risk in Review Study*; Base: 1,183

Q. With regards to the risk management function's performance today, to what extent do you agree or disagree with the following statements?

The risk management function helps increase the odds of success or decrease the odds of failure across the business.

And Adapters anticipate better results. They're nearly twice as likely to say their risk management function helps boost the odds of success—or reduce the odds of failure—across the business (Figure 1). Adapters who also consider their organization to be more innovative than their peers' organizations are three times more likely than their less-effective and less-innovative peers to anticipate revenue growth.

Our finding is consistent with recent research by Northwestern University's Kellogg School of Management, published in *Harvard Business Review*, which suggests that innovation, effective risk management, and growth go hand in hand. The article, titled "Data from 3.5 million employees shows how innovation

really works", which analyzed data on the ideation rates and profitability levels of 154 companies over five years, reports that profitability was higher among organizations that generated better ideas—most likely because the organizations had constructs to act on and manage ideas.¹

2018 Risk in Review Study sheds light on the current landscape of innovation and shows how risk management practices need to change if organizations are to capture value from new technologies and novel initiatives. Our report is also a bridge to PwC's *2018 State of the Internal Audit Profession* and *State of Compliance* studies because the lines of defense are now so interconnected and face similar innovation-related challenges.

¹ Dylan Minor, Paul Brook, and Josh Bernoff, "Data from 3.5 million employees shows how innovation really works." *Harvard Business Review*, October 9, 2017

The state of innovation and the changing risk landscape

With innovation and growth so tightly linked, it's no surprise that nearly 9 in 10 organizations are innovating in at least one of eight ways—or say they plan to do so by 2020 (Figure 2). And because technology underpins innovation in all forms, it's also no surprise that the top two of those initiatives are implementing new technologies to *improve* existing products (86%) and to *create* new ones (80%).

Respondents single out big data and the cloud as the technologies their organizations use or plan to use by 2020 that will most impact their organizations over that time. Artificial intelligence (AI) and the Internet of Things (IoT) deployments are also under way or planned and are expected to make an increased impact in the coming years, as organizations embrace the potential of those technologies. PwC projects that AI will add US\$15.7 trillion to global GDP by 2030 as a result of efficiencies and higher customer value.²

Changing an organization's talent model is third most prominent among innovative activities under way today or planned (70% of respondents).

As organizations push forward with technology deployments, skills too, need to change; and that necessary change is upending how and from where organizations source, develop, and retain talent. This priority follows years of organizations' neglecting to upskill their workforces while singularly focusing their attention on technology rollouts, according to PwC's Digital IQ[®] survey.³

Cyber and talent risks are top risks rising with innovation

Which risks associated with innovation are most acute? CEOs⁴ and risk analysts rank cyberthreats⁵ as a top risk to growth in 2018 globally. And yet PwC's Global State of Information Security[®] Survey finds that businesses are ill prepared for continually rising and evolving cybersecurity or privacy threats.^{6,7}

Perhaps that's why cybersecurity or privacy threats is seen as the risk category expected to rise the most with any form of innovation we queried. From introducing new products to entering new markets, to forming alliances, to creating new distribution models, cybersecurity or privacy is of greatest concern. As businesses operate in an increasingly digital world, technology underlies many innovative activities and, by extension, opens the door to greater cyber risk.

Take Bitcoin, which helps companies boost profit margins by reducing the number of necessary intermediaries. But cryptocurrencies like Bitcoin come with many risks. Users interact with unique, time-stamped tokens, each of them overseen by their own sets of software engineers who have mixed levels of security behind them. It's a shift from financial institutions serving as stewards of trust.⁸

- 2 [“Sizing the prize: What’s the real value of AI for your business and how can you capitalise?”](#) PwC, 2017
- 3 [“A decade of digital: Keeping pace with transformation.”](#) PwC, 2017
- 4 [“US business leadership in the world in 2018.”](#) PwC, January 2018
- 5 Sy Mukherjee, [“These are the biggest risks for businesses in 2018, according to the World Economic Forum.”](#) *Fortune*, January 17, 2018
- 6 [“The Global State of Information Security Survey[®] 2018.”](#) PwC, 2018
- 7 [“Revitalizing privacy and trust in a data-driven world.”](#) PwC, 2018
- 8 Jessica E. Lessin, [“The simple thing people miss about cryptocurrencies.”](#) *The Information*, December 8, 2017

Figure 2: Innovative activities under way or planned by 2020



Doing today



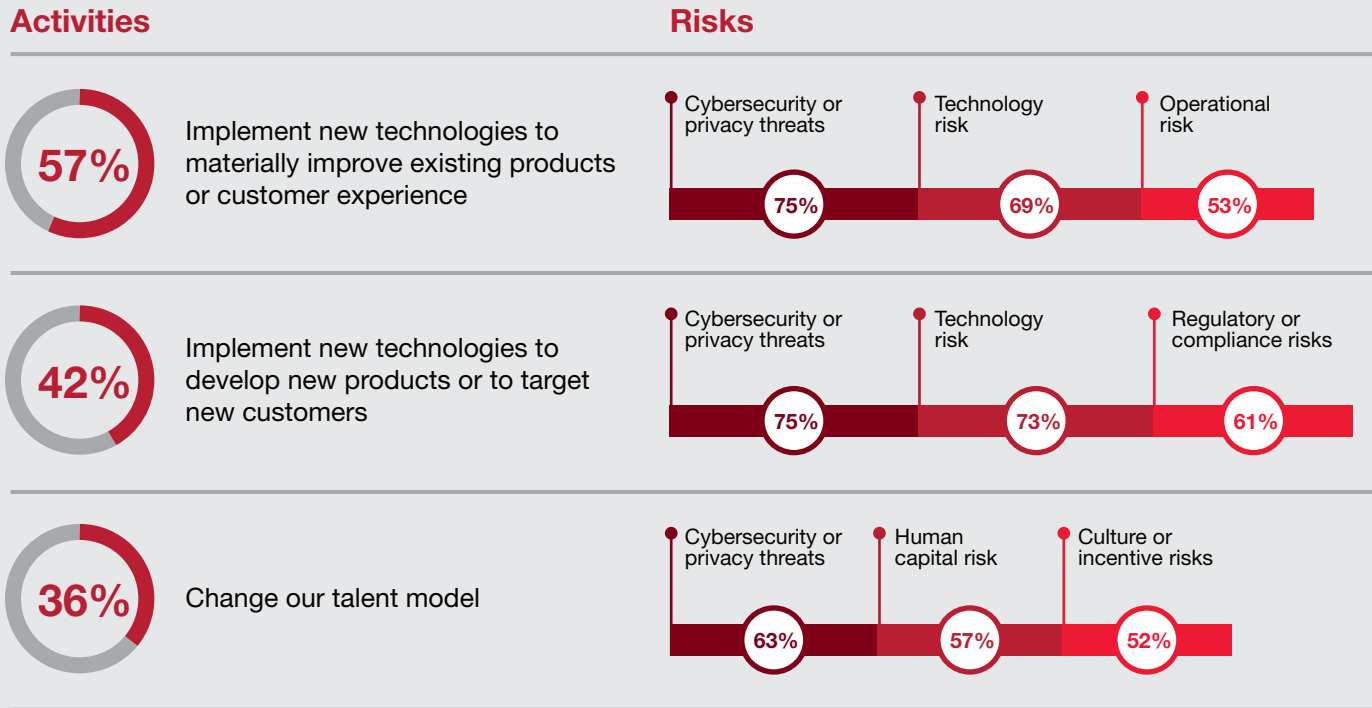
Within 3 years



Source: PwC, 2018 Risk in Review Study; Base: 1,543

Q. Which of the following innovative activities is your organization undertaking today or does it plan to undertake?

Figure 3: The three most critical innovative activities bring increased risks



Source: PwC, 2018 Risk in Review Study; Base: 527
 Q. Which of the following activities underway or planned at your organization has your leadership identified as most critical to your organization’s strategy?

Source: PwC, 2018 Risk in Review Study; Base: 831
 Q. For the three innovative activities you selected, do you believe each risk listed will increase or decrease in the next 3 years? (Top three of 12 increased risk responses listed)

As for IoT, many welcome cost and time gains from IoT and smart offices, plants, or ports. But the growing quantity of IoT devices—set to more than triple to 20.4 billion in 2020 from 6.4 billion in 2016, according to research firm Gartner⁹—raises concerns about weak security links that could open up control rooms, data vaults, and critical infrastructure to hackers. The oil & gas industry, for example, is a top target for cybercrime, with nearly 7 in 10 respondents reporting security breaches over the past year.¹⁰ Given some \$10 billion in energy infrastructure damage from Hurricanes Rita and Katrina in 2005,¹¹ the costs of a sophisticated and extended attack on refineries could be substantial, not counting casualties or reputational harm.

Emerging-technology deployments affect entire organizations. So, in addition to cyber and privacy risks, respondents cite many other risks linked to technology—such as regulatory, compliance, human capital, operational, culture, and incentives risks—as rising from the innovations most critical to their organizations’ strategies (Figure 3).

AI, for example, can dramatically cut the cost of talent searches, but its algorithms might be biased and thereby bring about outcomes based on assumptions that do not reflect reality. This concern preoccupies human resources and legal executives—among those in other functions—because their organizations’ hiring decisions could be based on embedded, biased AI filtering.¹²

- 9 “Gartner says 8.4 billion connected ‘things’ will be in use in 2017, up 31 percent from 2016.” Gartner press release, February 7, 2017
- 10 Collin Eaton, “HACKED, Part 1: As cyberattacks become more sophisticated, energy industry’s controls provide an alluring target.” *Houston Chronicle*
- 11 Michael Isaac Stein, “After Harvey, what will happen to Houston’s oil industry?” *WIRED*, September 21, 2017
- 12 Dina Bass and Ellen Huet, “Researchers combat gender and racial bias in artificial intelligence.” Bloomberg Technology, December 4, 2017

Effective risk management programs: Key attributes

When organizations respond well to the range of innovation risks like those identified in our study, it naturally follows that their innovations would be more successful. Survey respondents agree. Adapters more often (1) call their organizations *innovative*, (2) anticipate revenue growth, and (3) report that their risk management programs contribute significant value to their organizations (Figure 4). As Jerome T. Lienhard II, chief risk officer at SunTrust Banks puts it, “As a CRO, I have to think of opportunity cost. There’s an opportunity cost to not taking enough risk.”

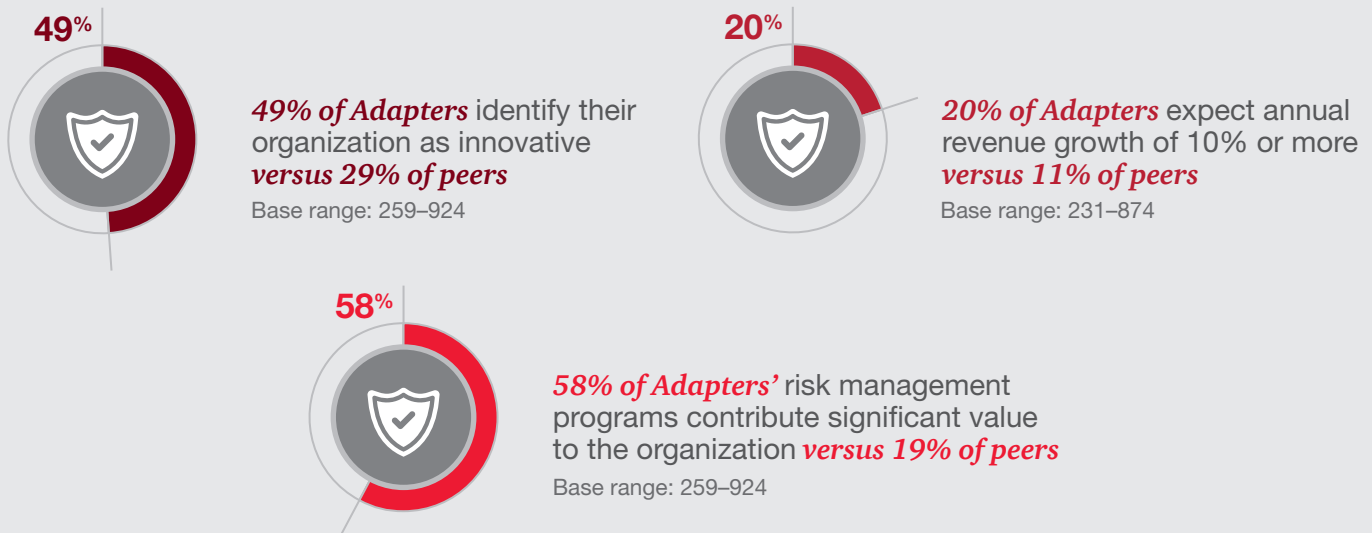
Adapters differ significantly from their peers in a few major ways, led by their higher level of confidence in their risk program’s ability to effectively manage technology risk.

That may be in part because a greater percentage say they provide input on innovation strategy and have influence over innovation-related decision making. Such involvement helps risk executives make sure strategy-related risks are known and that the program’s risk appetite is appropriate.

Confidence in the age of big data and artificial intelligence

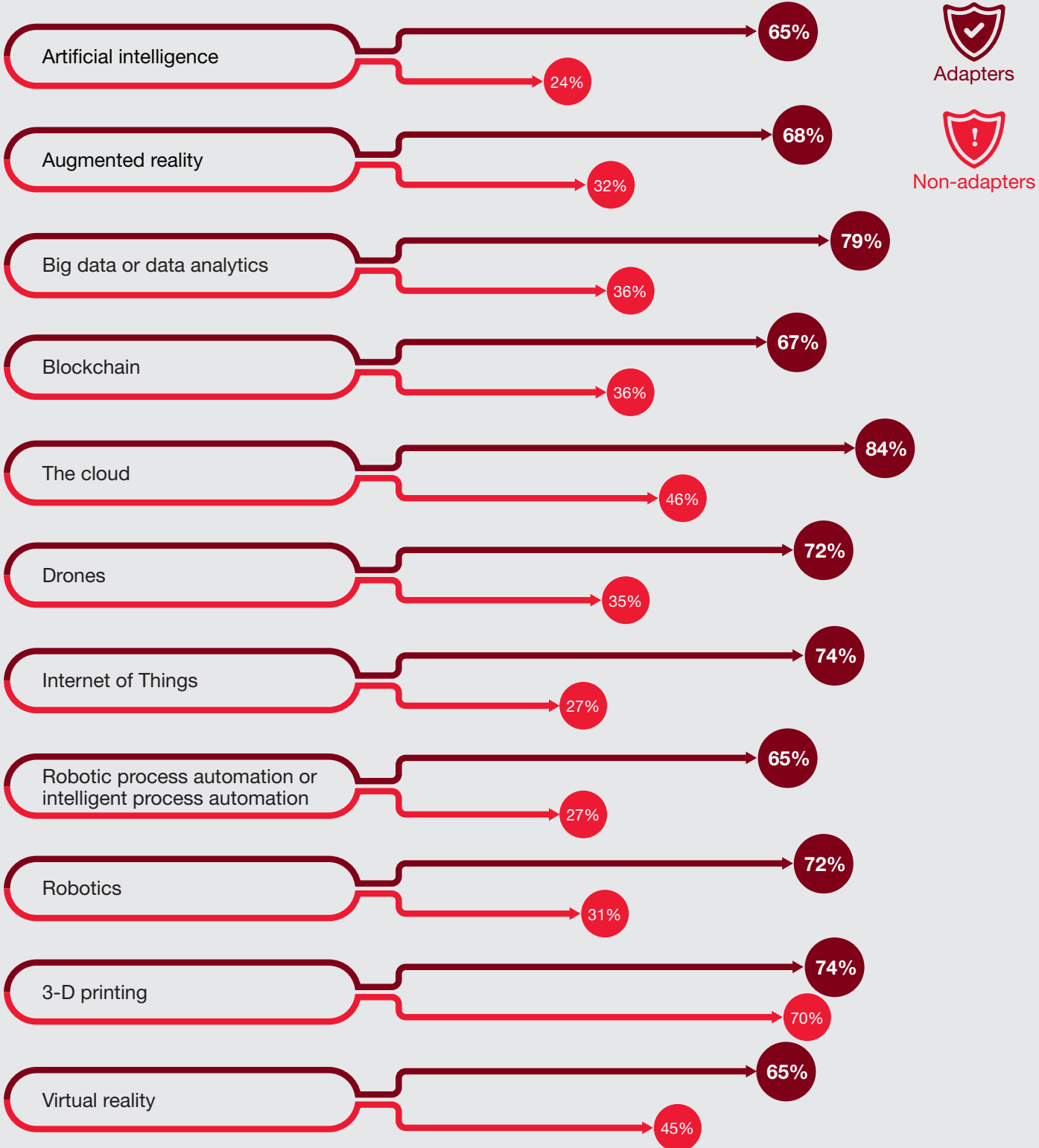
Notably, the percentage of Adapters that express confidence in their risk management program’s ability to effectively manage risks from AI, augmented reality, big data, IoT, and robotic process automation is at least double that of their peers (Figure 5). This is a significant advantage as emerging-technology deployments accelerate.

Figure 4: How Adapters stand out



Source: PwC, 2018 Risk in Review Study

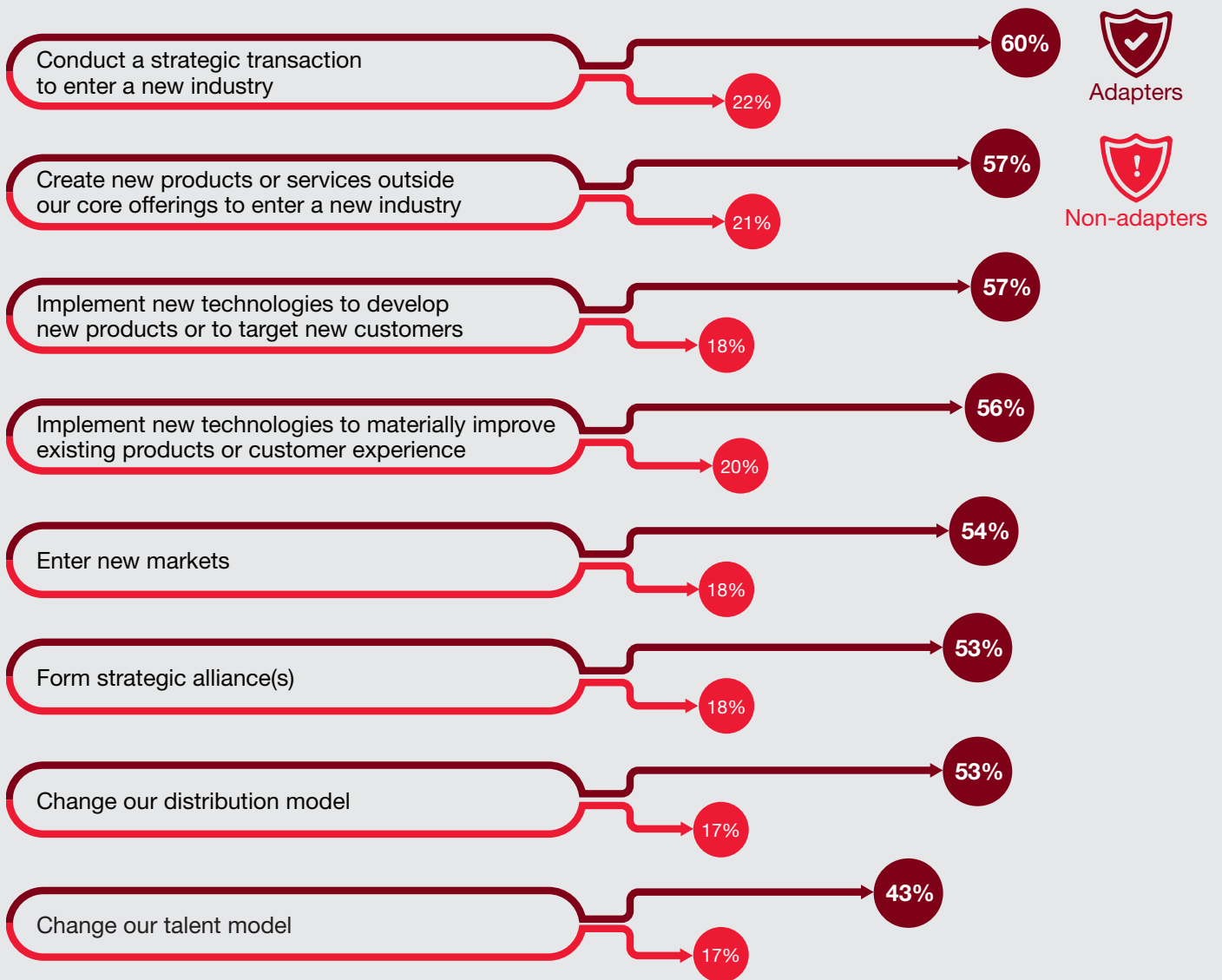
Figure 5: Higher confidence in program's ability to effectively manage AI, IoT, robotics risk



Source: PwC, 2018 Risk in Review Study; Base range: 133-1,103

Q. How confident are you in the ability of your organization's risk management program to effectively manage risks associated with the new technologies you identified as significantly impacting your organization?

Figure 6: Risk management program's ability to influence decisions about innovation



Source: PwC, 2018 Risk in Review Study; Base range: 522–1,036

Q. What is your risk management program's level of influence and ability to effect a change in decision-making about the listed activities?

Influence over decision making and the shaping of innovation strategy

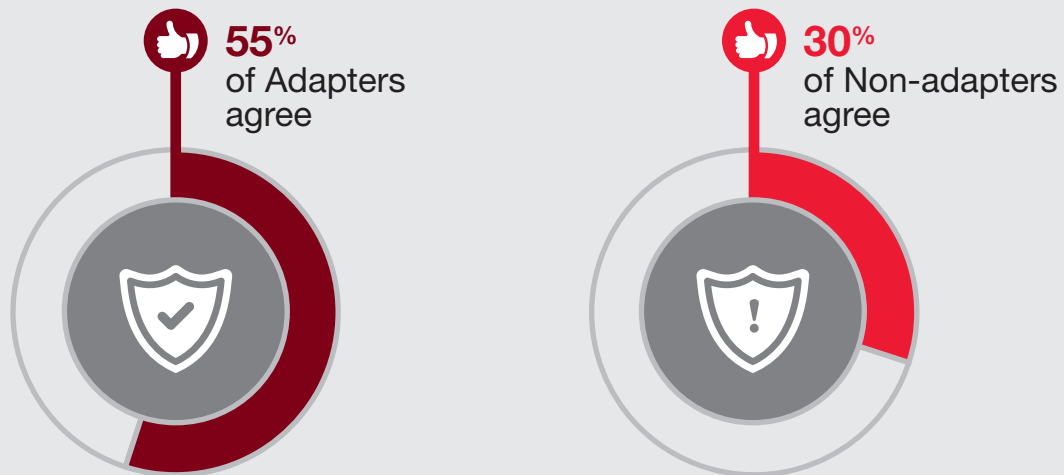
Adapters also exert more influence over decisions about innovative initiatives, with double to triple the percentage of their less-effective peers making that

claim. More than 50% of Adapters say their programs influence and effect change in decision making in seven of eight innovative activities we queried (Figure 6). Adapters are also nearly twice as likely to say that the risk management function provides strategic advice and helps shape innovation strategy and execution (Figure 7).

“Innovating requires risk taking. If you have a strong risk management capability, then you can create the space or opportunity for the innovation to occur.”

—Jerome T. Lienhard II, Chief Risk Officer, SunTrust Banks, Inc.

Figure 7: Risk management function’s influence on innovation strategy and execution



Source: PwC, 2018 Risk in Review Study; Base: 1,183 (Responses exclude disagree and neither/nor.)

Q. With regards to the risk management function’s performance today, to what extent do you agree with the following statement?
The risk management function provides strategic advice and helps shape the innovation strategy and execution.

Actions of effective risk management programs: Identifying, assessing, and adjusting for risk differently

Exerting influence over decisions about innovation positions risk executives to help their organizations understand—and therefore better manage—innovation-related risk.

But what underpins that position of influence? Adapters' risk management programs stand out in several ways. They are more often involved early in the innovation cycle; they use a broader range of actions to address their exposure to innovation-related risk; they more often adjust risk appetite and tolerances to align with strategic objectives; they're more often equipped with the expertise and tools to assess innovation-related risks; and they measure and monitor risk management effectiveness from multiple angles.

Engage early and often across the innovation cycle

Risk executives must weigh in very early about novel initiatives as the pace of innovation accelerates and the appetite for the accompanying

risks grows. Thus, Adapters and their risk management programs differ in *when* and *how* they engage in innovative activities.

Adapters play a more active role across the innovation cycle; they're twice as likely to say they advise on innovative activities before the planning stage; and they're much more likely to say they halt initiatives based on risk assessments and suggest risk-based alternatives (Figure 8).

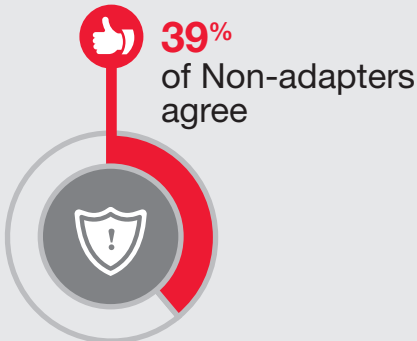
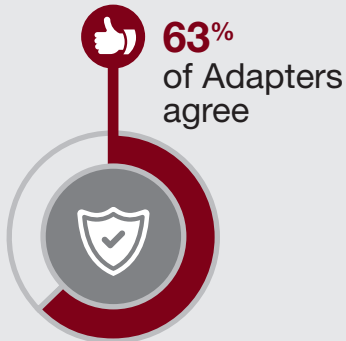
Risk assessing opportunities at inception and making critical go-no-go decisions jointly with the business along the way help keep innovation-related risks at the forefront throughout the innovation cycle. (See "Assessing risk in the sandbox.")

These findings fortify findings by other studies¹³ that show that organizations manage risk more effectively if senior risk executives are (1) involved in high-level strategizing with business leaders and the board about new investments and (2) more attuned to risks in internal and external operations. Without such deep involvement, risk executives are more likely to resist otherwise promising innovations or be blindsided by critical risks.

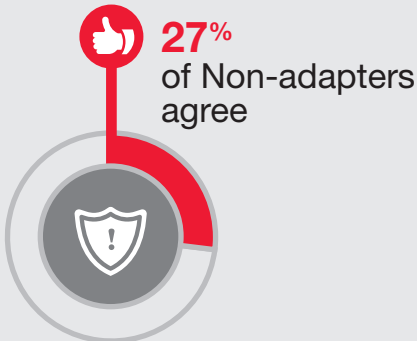
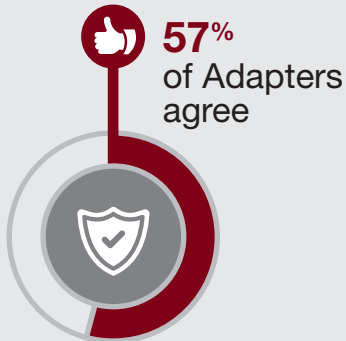
13 Gary Perlin and Kenneth M. Eades, "The business of risk: a CFO's view of risk management," *Darden Ideas to Action*, September 5, 2017

Figure 8: Adapters and their programs differ in when and how they engage in innovation

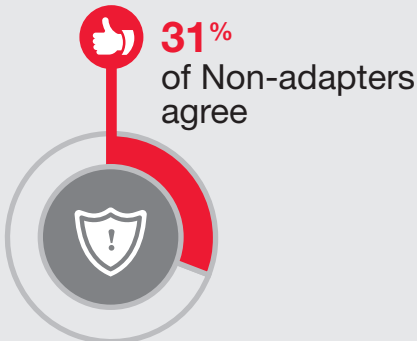
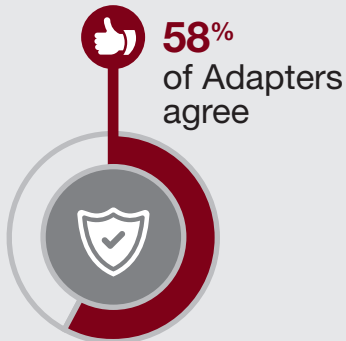
The risk management function can halt specific initiatives, based on its risk assessment



The risk management function provides input when an innovative activity is considered, before the planning stage



The risk management function proposes risk-assessed alternatives to specific activities

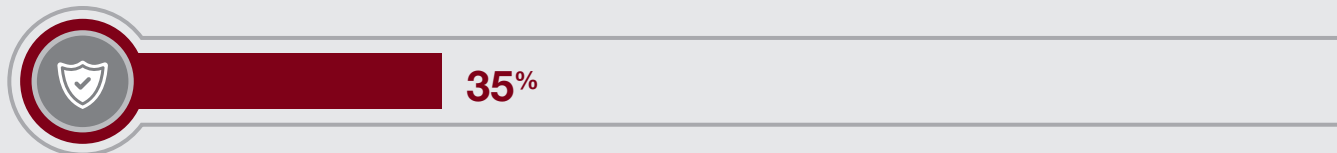


Source: PwC, 2018 Risk in Review Study; Base: 1,183 (Responses exclude disagree and neither/nor.)
 Q. With regards to the risk management function's performance today, to what extent do you agree or disagree with the following statements?
 The risk management function can halt specific initiatives, based on its risk assessment
 The risk management function provides input when an innovative activity is considered, before the planning stage
 The risk management function proposes risk-assessed alternatives to specific activities

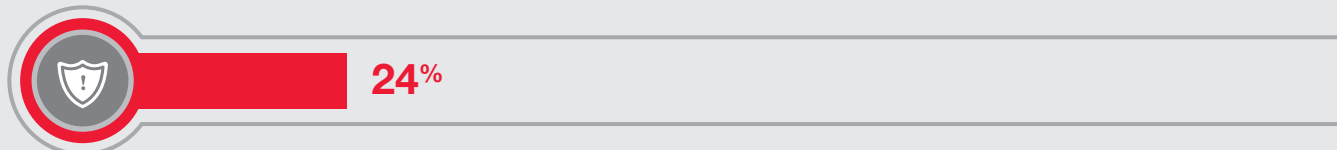
Figure 9: Adapters more often take multiple actions to manage innovation risk exposure

4 or more actions taken

Adapters



Non-adapters



Actions

- Accepted the risk
- Adjusted the risk appetite
- Postponed the activity to avoid assessed risk
- Reduced the risk
- Revisited the objectives and strategy
- Shared the risk

Source: PwC, 2018 Risk in Review Study; Base range: 220–830

Q. Which of the following actions has your organization undertaken to manage your organization’s risk exposure from the innovative activities you selected?

Adobe knows this. The company, which ushered in the desktop publishing revolution in the 1980s, has since evolved into a top provider of software and cloud-based services. That business transformation brought enormous strategic and operational risk as the organization migrated customers to cloud-based from on-premise applications, led by potential customer flight from possible service failure.

Today the firm recognizes that its success in providing such services depends on, for instance, its ability to prevent outages. “As a cloud-service provider, you’re looking at 99.99% availability,” Eric Allegakoen, vice president of Global Audit & Business Assurance (CAE) at Adobe, told us in an interview.

Take multiple actions to manage risk exposure

In addition to early involvement in the innovation cycle, Adapters take a number of approaches to manage risk exposure. They’re nearly one and a half times more likely to take multiple actions (four or more) to reduce risk exposure from the eight innovative activities we investigated (Figure 9).

Assessing risk in the sandbox

To influence decisions about innovation, risk executives are increasingly playing a sandbox-monitoring role. They're chiming in early on innovation discussions, letting business leaders test-drive novel initiatives both before and after launch to work out the risk glitches, and advising on how to prepare for and address risk well before a new product or service launches.

They're clearing a path and creating a safe and transparent space to ideate and implement novel ideas—a space where onerous and perhaps unnecessary rules won't stifle innovation. For example, Legg Mason “had to let some things go out of the sandbox and breathe,” the company's Chief Risk Officer, Joe Carrier, told us referencing newly created add-ons to its automated investing system. However, he added, “We have folks ‘riding-along’ to make sure we build the appropriate protections, controls and infrastructure around it.”

Advisors in the asset management firm's sandbox include a risk representative, a compliance professional and members of the resiliency teams. The team involved is fully transparent. “We are doing some of these things without knowing precisely what the outcomes will be in the long term but having some trust there are enough eyes on it,” Carrier said.

“Innovation risk is a strategic question. The risk of not innovating is just as high as the risk of innovating, if not higher.”

—Kimberly Johnson, Chief Operating Officer, Fannie Mae

Adjust risk appetite and tolerances with frequency

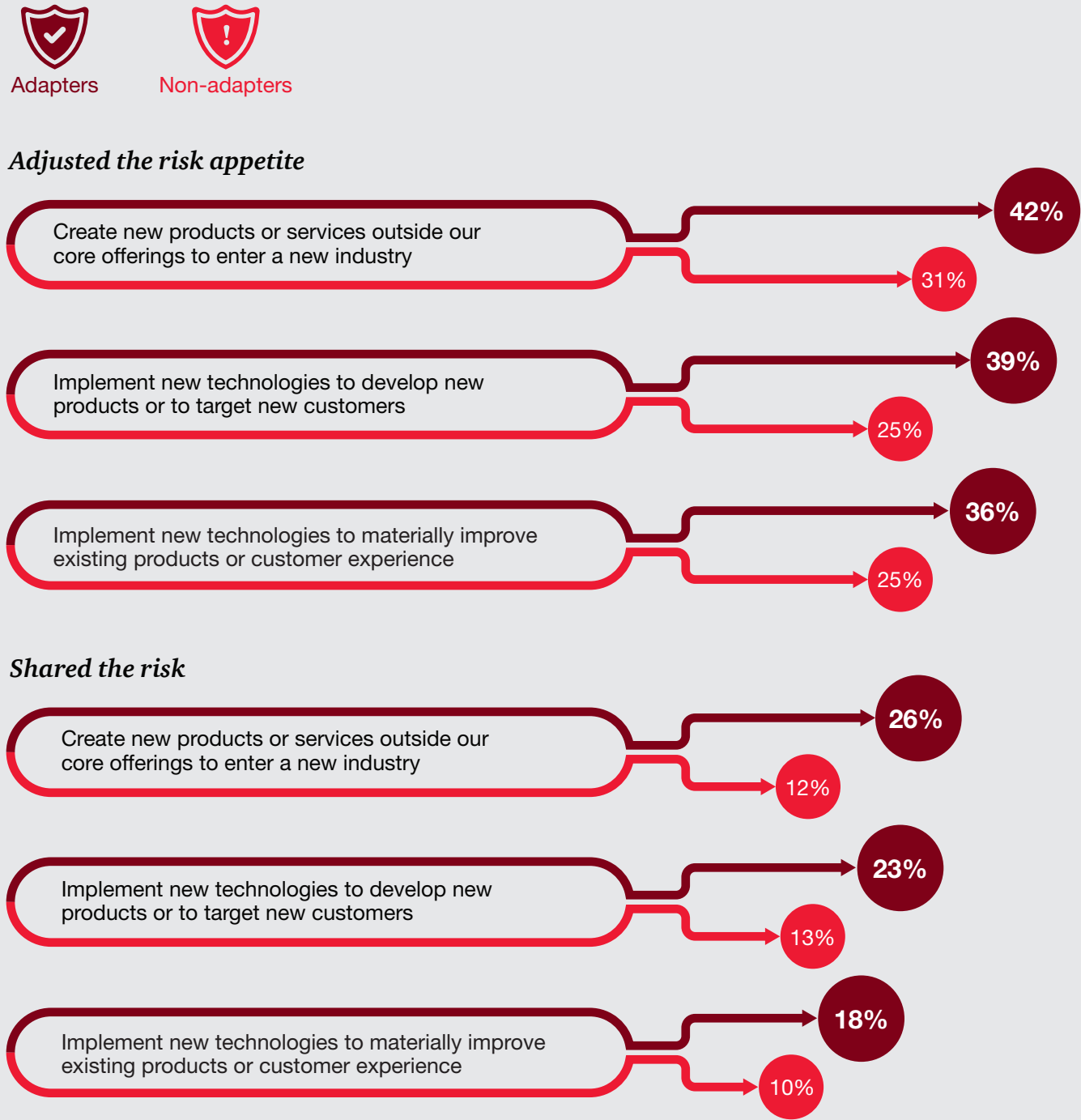
Given today’s focus on capturing value from emerging technologies while closely tracking risk, quick, calibrated, and disciplined adjustments to risk appetite and tolerances are critical.

An organization’s risk tolerance for innovation for instance, may be quite different from its compliance risk tolerance or cybersecurity risk tolerance. And its overall risk appetite may need to shift over time due to market direction or competitive dynamics. It’s also important to continuously communicate such changes to the C-suite, the board, internal auditors, and the business so those parties can act on incoming data.

Considering this, it’s no surprise that Adapters more often say they adjust their risk appetite and share the risks they encounter as they pursue various innovations (Figure 10). Those adjustment and sharing actions are particularly prevalent as their organizations implement new technologies or create products that are outside their core offerings. This makes sound business sense as different sectors increasingly partner to deliver digital services, operations, or models.

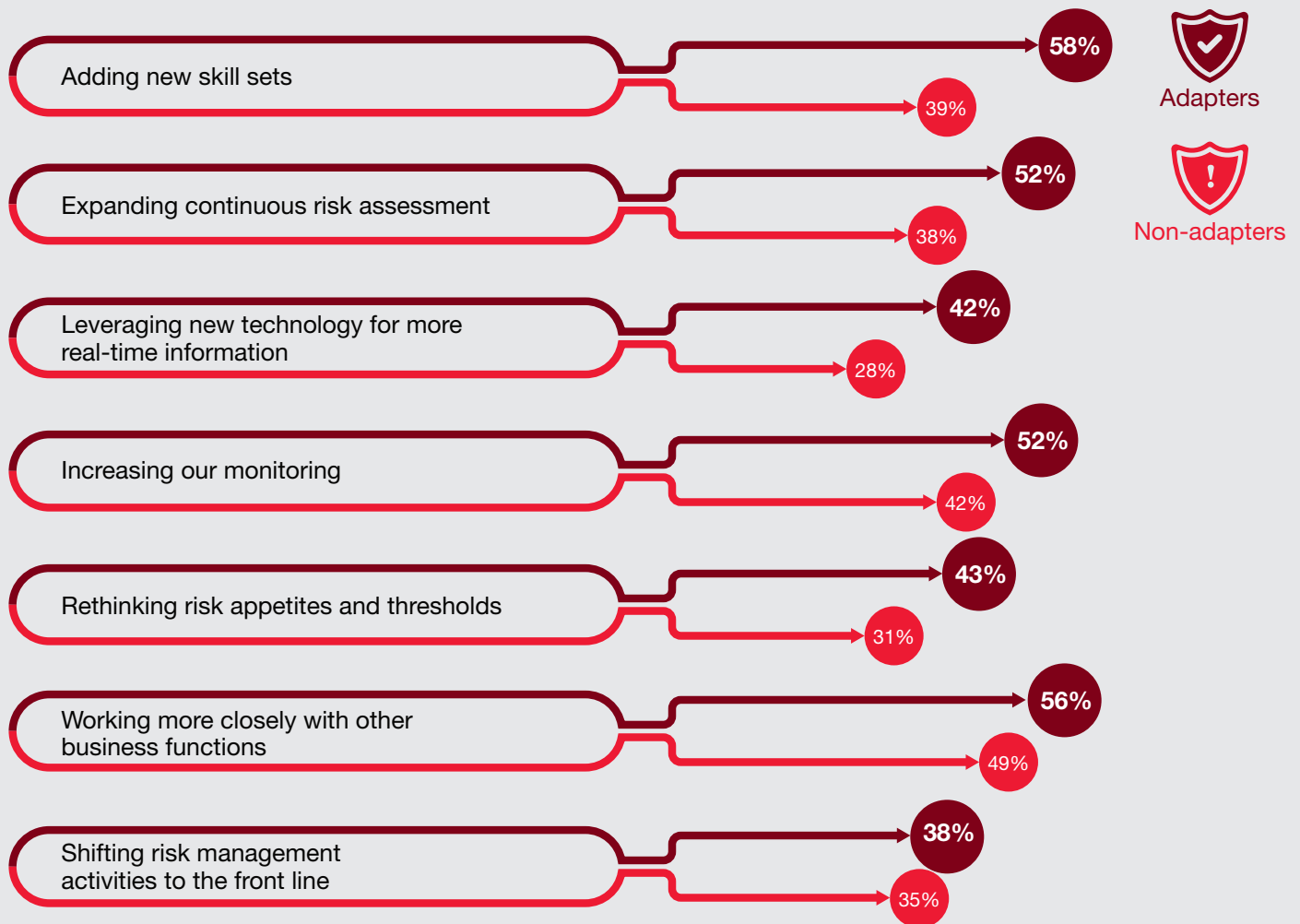
As an organization periodically adjusts its risk appetite and tolerances, all lines of defense should be informed of such changes so that business decisions, controls testing, risk monitoring, and risk reporting work in a synchronized and risk-aligned manner. Such alignment was explored in last year’s *Risk in Review Study*.

Figure 10: Adapters more often adjust their risk appetite and share the risk



Source: PwC, 2018 Risk in Review Study; Base range: 177-644
 Q. Which of the following actions has your organization undertaken to manage your organization's risk exposure from the innovative activities you selected?

Figure 11: How risk executives are adapting capabilities to support innovation strategy



Source: PwC, 2018 Risk in Review Study; Base: 1,183
 Q. How are you adapting your risk management capabilities to more effectively influence and enable your organization’s innovation strategy?

Harness new skills, new competencies, and new tools to support innovation

To adapt their capabilities to influence and enable their organizations’ innovation strategies, Adapters are much more likely to say they add new risk-related skill sets, expand continuous risk assessment, and use new technology for more real-time information (Figure 11).

It’s not surprising that adding new skills is the top change Adapters are making. Digital workforce transformation requires new knowledge, new skills, and an entirely new mind-set, which are daunting for many and takes time.¹⁴ In fact, more than 80% of CEOs we polled in PwC’s *CEO Survey* say even their own soft and digital skills need to improve.¹⁵

Our *2017 Digital IQ Survey* also found that nearly two in three (63%) of 2,200 business and IT leaders we queried called the lack of skilled teams their top obstacle to digital innovation.

¹⁴ “A decade of digital: Keeping pace with transformation.” PwC, 2017

¹⁵ “US business leadership in the world in 2018.” PwC, January 2018

Many companies lack these capabilities. Adding knowledgeable, curious, action-oriented, and tech-savvy recruits is critical if an organization is to keep pace with risks from technology-driven innovation. But organizations can't only hire their way into the future; their current workforces will require upskilling in new methods, metrics, tools, and technologies to make critical, in-the-moment risk-reward decisions.

The priority on skills found in our study dovetails with that of our *2018 State of the Internal Audit Profession Study*, which found that 72% of Evolvers—or organizations where internal audit is most advanced in its use of technology—excel at obtaining, training, and sourcing of the talent they need, versus 29% of Observers, which are organizations that most lag in their adoption of technology. Internal audit functions that are the most mature in their technology use are progressing their technology and talent in lockstep and delivering more value to their organizations.

Arming the risk management program with tools to rapidly spot, assess, and react to digital risk as well as with technologies that make real-time communication and collaboration possible are important components

of effective risk management. Such tools granularly quantify opportunities and risks—particularly from new and poorly understood technologies—and they track and push risk appetite and tolerance changes across the organization. Data analysis and visualization tools are essential in this endeavor.

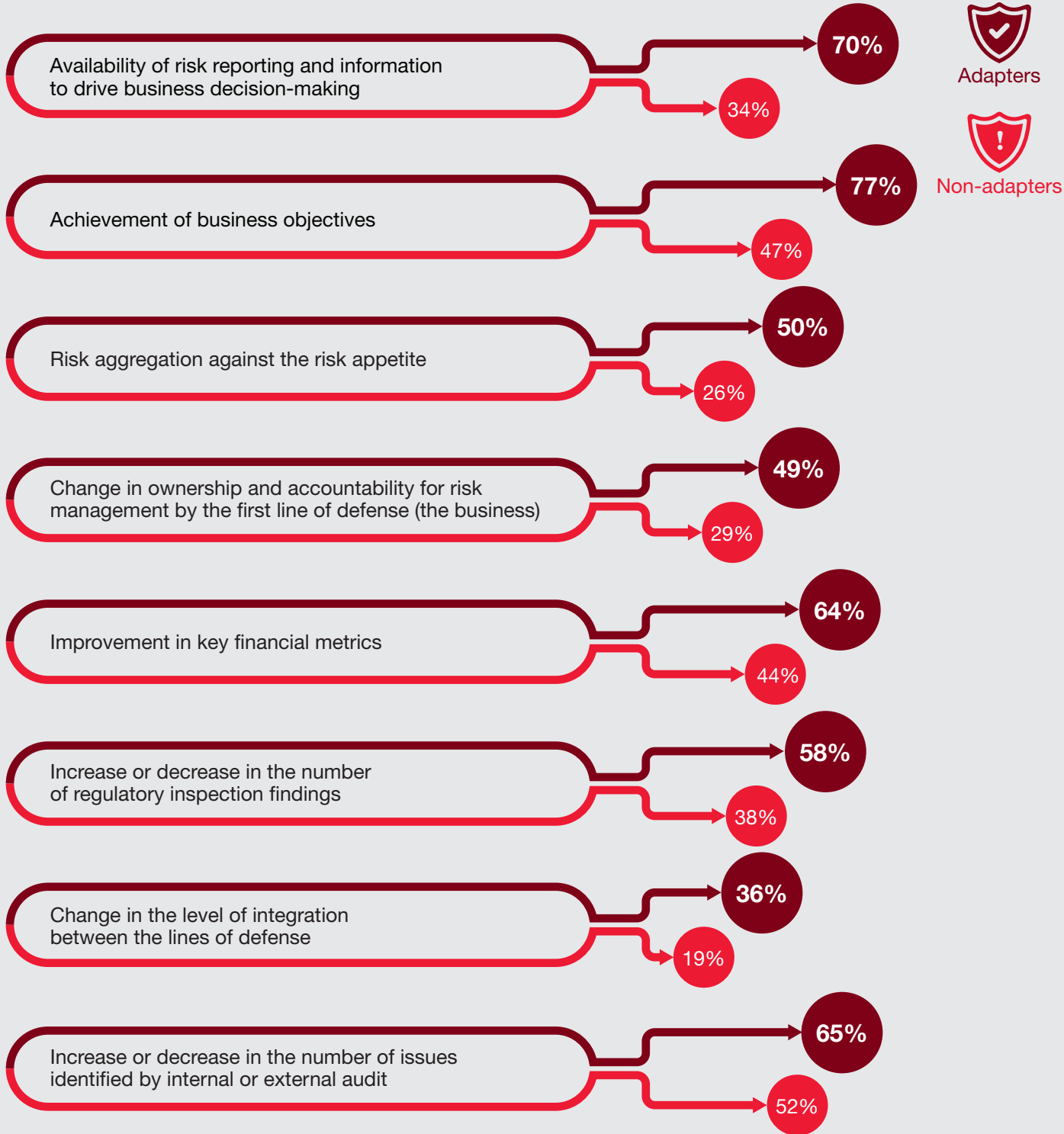
Monitor and assess effectiveness of risk management in multiple ways

The rigor and frequency with which risk executives assess their organizations' risk management effectiveness reflect how serious the organization and the risk function are about tracking and addressing rapidly arising risks.

Much more often, Adapters say they use five or more of the eight metrics we queried (55% versus 24%) to measure the effectiveness of risk management.

The biggest gaps between Adapters and their peers are in their uses of achievement of business objectives, availability of risk reporting information, and risk aggregation against the risk appetite as key performance metrics (Figure 12).

Figure 12: Metrics used to measure effectiveness of risk management activities

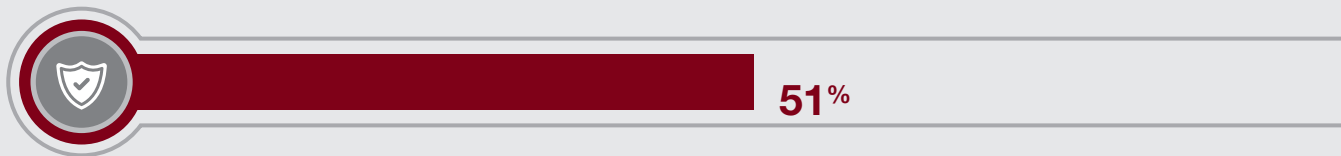


Source: PwC, 2018 Risk in Review Study; Base: 1,183
 Q. Which financial or operational metrics does your organization use to measure the effectiveness of its risk management activities?

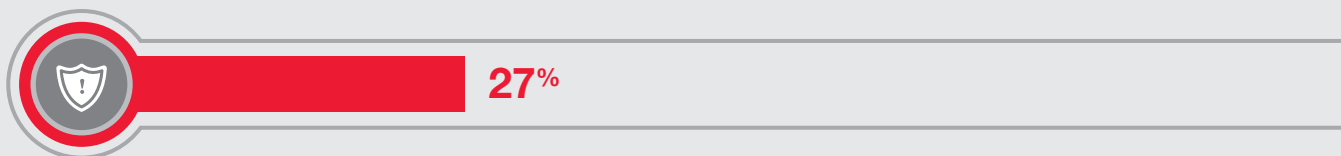
Figure 13: Mechanisms most used to measure effectiveness of risk programs

Assessment of risk management capability by external parties

Adapters

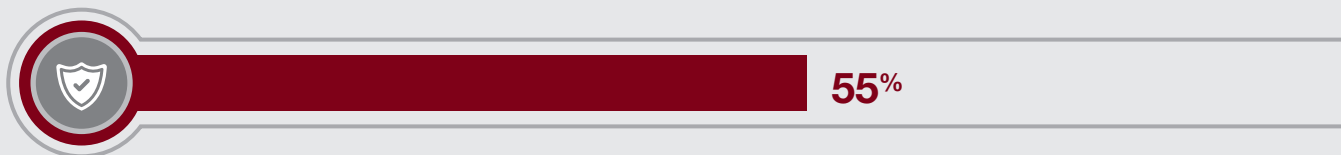


Non-adapters

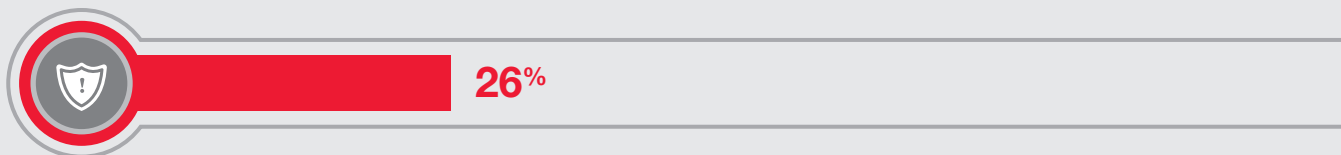


Regular assessment of the capabilities of the second-line risk management function

Adapters



Non-adapters



Source: PwC, 2018 Risk in Review Study; Base: 1,183

Q. Which of the following mechanisms does your organization use to monitor the effectiveness of its overall risk management program?

Examining effectiveness through multiple metrics can help risk executives shore up areas where they fall short or are vulnerable, so that the C-suite and the board can rapidly make decisions about strategic initiatives while the business steps in to address any risk profile misalignments against risk appetite. The achievement of business objectives as a top metric demonstrates the importance of

alignment of risk to strategy in the management of innovation risk.

A striking difference between the Adapters and non-adapters is that the Adapters much more often use external assessment of risk management's effectiveness. They are also twice as likely to say their organizations regularly assess the capabilities of second-line risk management functions (Figure 13).

As organizations embrace innovation, risk management programs can achieve greater visibility, better efficacy, and avoided cost gains by monitoring the effectiveness of their risk management through multiple means. Doing so helps make sure that the right controls are in place and that the right actions are taken—at all levels.

The way forward: Obstacles to clear

The relentless pace of change can blur many organizations' visions of how to improve innovation risk management. "It's more difficult to see what's around the corner when innovations are happening at lightning speed," said

Johnson of Fannie Mae. Indeed, when asked to describe their visions of the future risk management function, respondents most often chose the word "challenging" (Figure 14).

Figure 14: The future of risk management in one word



Source: PwC, 2018 Risk in Review Study; Base: 1,258

Q. As you envision the future of your risk management function, please supply one adjective to describe that vision.

What are the biggest obstacles? Non-adapters suggested organizational culture as the top obstacle to more effectively managing innovation-related risks (Figure 15). In this context, *culture* means *risk culture*, which in many organizations is undergoing dramatic change as staff shift to digital ways of working.

The appropriate risk culture starts at the top as the CEO sets the tone for risk management to be involved in all facets of critical innovation-related decisions across the organization. With the right risk culture, risk management programs become well equipped to tightly link risk to strategy and to connect performance metrics to the effective management of innovation risk.

Other obstacles holding back the less-effective cohort are (1) lack of knowledge of innovation-related opportunities and risks, which is not surprising, given the speed of change; (2) lack of leadership buy-in, which limits risk management's power; and (3) weak collaboration with the business, which might span time zones and levels.

The choke point for effective risk management is often at lower or local organizational levels. Consider the bank branch manager who fails to receive vital, risk-linked information because he or she missed the latest town hall,

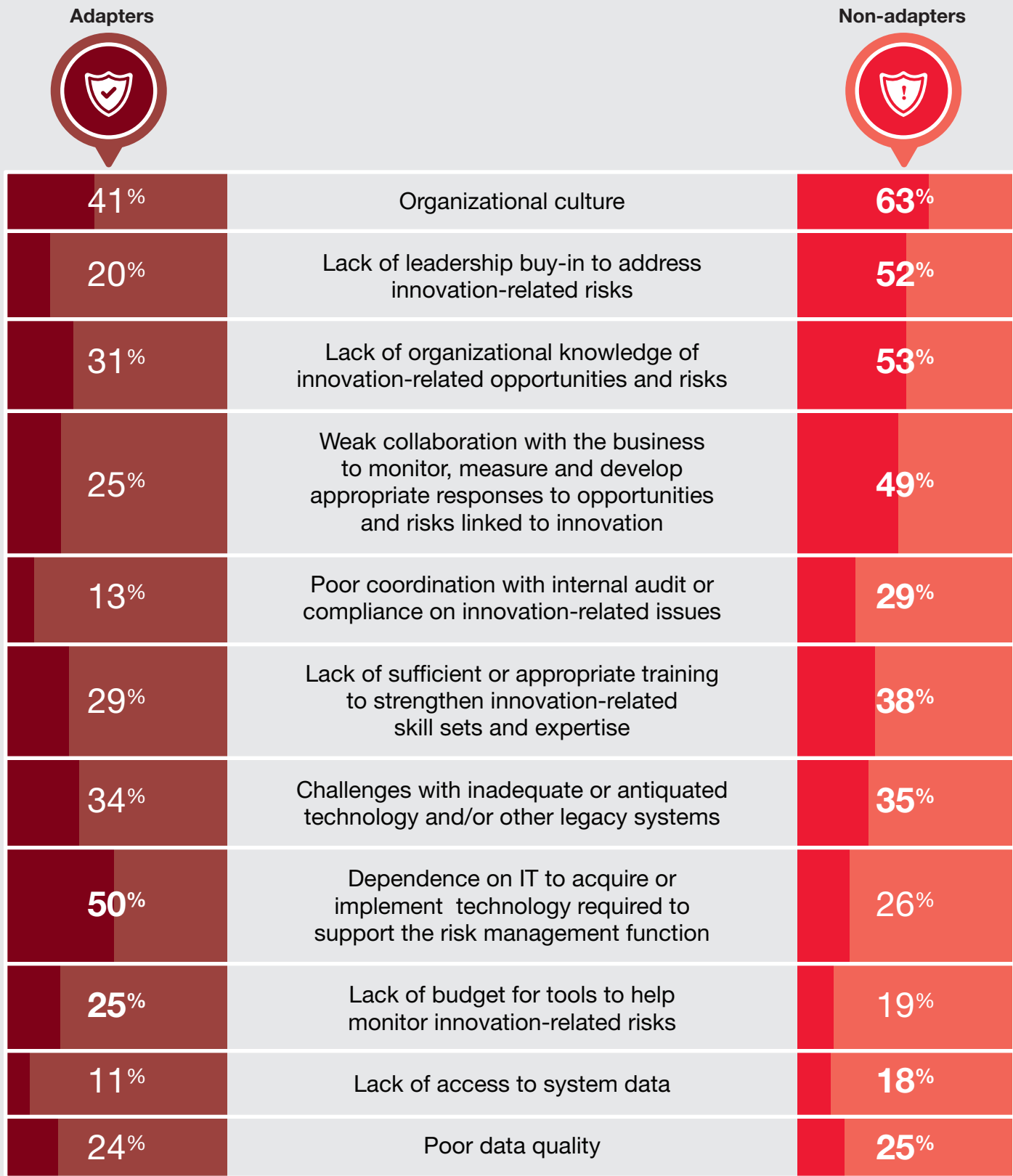
or the subsidiary lead abroad who hatches risky incentive-based schemes to meet overly ambitious growth goals.

To spot risk and react at the right time in the right manner, making sure important messages cascade across and into the crevasses of an organization, is critical. PwC calls this *tone at the middle*.

Fostering a strong risk and teaming culture is not easy. The often-disintegrated nature of the three lines of defense, the usual disconnects with the business, and limited resources get in the way. Groups like blended innovation committees with committed executives from risk, compliance, and internal audit, and C-suite and business leaders who meet regularly can help push successful management of innovation-related risk higher on the corporate and business agenda.

Companies are taking action. Cisco Systems Capital holds a quarterly risk council meeting where the president of the company reviews risk concerns and comments on strategic initiatives with senior leadership. The chief credit and risk officers discuss strategic initiatives at the executive level. Legg Mason's innovation council is sponsored by its CEO, and the group holds a monthly call, supplemented by ad hoc conversations, pilot projects and proof of concept implementations.

Figure 15: Obstacles to more effective management of innovation-related risks



Source: PwC, 2018 Risk in Review Study; Base: 1,183
 Q. Which, if any, of the following issues is preventing your organization from developing more effective risk management to respond to innovation-related risks?

“How do you empower people to take risks to innovate and take away their fear of being penalized for failures that are part of that innovation process? If you punish people for taking risks and hold them accountable for novel ideas failing, you’re going to stop getting novel ideas.”

—Jennifer MacKethan, Global Manager, Integrated Risk Management, Cisco Systems Capital

Fueling growth in the age of innovation

Organizations must view innovation and risk as a two-edged sword, clearing the way for greater opportunity and increased revenue growth, with eyes wide open about all-but-certain and unimaginable risk. To allow for more innovation and to deflect or limit risks from new initiatives as they arise, risk executives must be engaged and influential over the entire innovation lifecycle—from high-level strategizing to brainstorming, to quantifying, to executing, to continuously taking decisions and actions about risk appetite, to performance tracking. To play this important role, risk management programs must be equipped to effectively identify, assess, and manage innovation risk. Applying rigor, using

multiple approaches, pushing the organization to periodically adjust risk appetite, adding sophisticated skills and tools, and comprehensively monitoring how successfully the program is tackling innovation-related risk best help risk executives meet their organization’s strategic objectives.

When organizations effectively manage innovation-related risk, the likelihood they will be successful innovators rises. That simple premise is a call to action for risk management programs. As digital technology accelerates the pace of change, effectively managing innovation-related risk becomes crucial—and failure to innovate all but guarantees underperformance.

Five actions to take today

Drive risk tone and culture from the top

- Broadcast appetite and tolerance messages about innovation and risk across the organization, particularly to midlevel managers and regions where oversight and tone often collapse
- Tie effective management of innovation-related risk to strategic planning and performance management, thereby ensuring that risk behaviors are aligned, measured, and monitored

Engage early and often across the innovation cycle

- Champion risk executives as strategic contributors to innovation—from concept to rollout
- Push risk professionals to lean into innovation at the ideation stage, to assess risks, and to influence decisions about new initiatives
- Diversify and grow approaches for managing risk exposure, including sharing risk with partners, postponing initiatives while taking action to reduce risk, and halting initiatives when risk exceeds tolerance

Adjust risk appetite and tolerances with frequency

- Set risk appetite and tolerance for green-lighted innovation projects before launch, and periodically revisit the overall risk appetite to ensure it remains relevant and appropriate for the innovation strategy
- Ensure that adjustments to risk appetite are shared across the lines of defense so that business units, the risk and compliance functions, and internal audit are working in a synchronized and risk-aligned way

Harness new skills, new competencies, and new tools to support innovation

- Assess skills and competencies to prepare for and embrace digital innovation and to better—and more quickly—address associated risks
- Upskill resources in new methods, metrics, tools, and technologies
- Embed data analytics and visualization into the organization's risk assessment and management processes for early visibility into potential risks and for richer insights for risk monitoring and decision making

Monitor and assess risk management's effectiveness through multiple means

- Assess effectiveness with rigor and frequency by using multiple strategic and operational performance metrics
- Obtain a more honest picture of risk management's effectiveness through unbiased and objective metrics or sources

Risk in Review Study methodology

From October to December 2017, PwC surveyed 1,535 risk executives at organizations headquartered in 76 countries, and later interviewed 11 risk leaders across a range of industries; many of those leaders are quoted in this report. Further details by region and industry are available on request. Interviews were conducted in person and by phone.

Respondents primarily hold the titles of chief audit executive, general auditor, board member, audit committee member, audit committee chair, chief compliance officer, head of compliance, chief ethics and compliance officer, chief financial officer, chief executive officer, chief operations officer, chief risk officer, head of risk management, director of risk, chief information officer, and chief technology officer.

The lower size threshold for all companies included in the survey was annual revenue of \$499 million or less. The upper revenue threshold was \$5 billion or more.*

- 25% had revenues of \$499 million or less
- 37% had revenues of \$500 million to \$4.9 billion
- 35% had revenues of \$5 billion or more

Respondents work at organizations with headquarters in 76 countries.

- 35% North America
- 29% Europe
- 21% Asia Pacific, including India
- 8% Central and South America
- 7% Middle East and Africa

Respondents' employers represent 30 industries in 5 sectors.*

- 38% consumer industrial products and services
- 34% financial services
- 11% technology, information, communication, and entertainment
- 8% healthcare
- 7% government and public sector

*Not all figures add up to 100% because of the rounding of percentages and neither/nor and don't know responses.

The research for the study was undertaken by PwC Research, our global center of excellence for primary research and evidence-based consulting service. The base for all figures is 1,535 (all respondents) unless otherwise stated. For some questions in which the number of responses may vary, we provide a base range. This is often because response options branch from an earlier question and thus change the sample size per response.

Thank you to those who participated in the survey and to our clients who were interviewed for the Study.

To have a deeper conversation about how this subject may affect your business, please contact:

Brian Schwartz

*US Financial Services Internal Audit,
Compliance and Risk Management
Solutions Leader & US GRC Enablement
Solutions Leader*
brian.schwartz@pwc.com
+1 (202) 729 1627

Scott Greenfield

*Digital Risk Solutions and
Risk Assurance Innovation Leader*
scott.greenfield@pwc.com
+1 (646) 471 5383

Andrew McPherson

*Global Governance, Risk & Compliance
and Internal Audit Solutions Leader*
andrew.mcpherson@pwc.com
+61 (0) 418 431 296

Jason Pett

US Risk Assurance Leader
jason.pett@pwc.com
+1 (410) 659 3380

Jaime Phillips

*Director, Internal Audit, Compliance
and Risk Management Solutions*
jaime.d.phillips@pwc.com
+1 (703) 918 3008

Jim Woods

Global Risk Assurance Leader
jim.woods@hk.pwc.com
+1 (852) 2289 2316