KPMG

Disruption is the new norm

Tech risk management survey report

Forbes insights

kpmg.com

Table of contents

Foreword: Is disruption the new norm for technology risk?

"We are pleased to share with your our findings from our inaugural Tech risk management survey. As we consumed the data from the survey, one thing was absolutely clear: Traditional technology risk methods have evaporated and enterprises need to create an agile and dynamic technology risk organization to keep up with the pace of change. The question is, 'How?' Through this survey, we have attempted to shed light on some perspectives that leading organizations are taking to build a forward-looking technology risk organization."

–Vivek Mehta, Partner, KPMG LLP

Welcome to the fourth Industrial Revolution

Seizing control over the technology environment: It's absolutely vital, but consistently elusive. From banks, to hospitals, to manufacturers, to technology companies, that's the reality facing organizations in almost every industry today. Why?

For one, software and systems increasingly power the core activities of the business. Technology is embedded into most critical operating processes, supporting the work of both back- and front-end functions. That means the implications of mistakes, failures, or breaches can be severe from an operational, financial and reputational standpoint. A 2017 survey of more than 4,000 global CIOs by KPMG International and Harvey Nash found IT leaders are wholly focused on navigating uncertainty in light of political, business and social change. Adding to the uncertainty is the relentless rise of organizations being subject to "major" cyber attacks. In fact, cybersecurity vulnerability is now at an all-time high.[1]

Second, we are living in a disruptive world. Data is proliferating and technology is becoming more complex. From automation, to artificial intelligence (AI), to the Internet of Things (IoT), to big data, to customer-facing apps and digital services, the rapid pace of technological change represents one of the biggest threats to today's businesses.

[1] *2017 CIO survey (KPMG International and Harvey Nash, 2017)*

KPMG

KPMG's 2017 survey on the *Changing landscape of disruptive technologies* found that the following are the biggest barriers to commercialization:[2]

32% Risk management and cybersecurity

29% Regulatory compliance

29% Privacy governance

Also, it was noted that AI, cognitive computing, IoT and robotics are the top three technologies that will drive business transformation in the next three years.[2] Within organizations, this rapid evolution of technology is pushing technology risk into the limelight and raising the profile of the technology risk management function[3]—from server rooms to boardrooms.

In light of this challenging landscape, KPMG LLP (KPMG) set out to explore the current state of technology risk across industries. We surveyed more than 200 executives about key issues in the field, including how technology risk leaders:

- Deal with emerging technologies and technological complexity
- Identify, manage and measure technology risk proactively
- Transform technology risk from cost centers to strategic value drivers

Featuring proprietary research brought to life by astute perspectives from KPMG specialists, this report distills key findings from the survey in order to unveil insights into next-generation approaches to technology risk—best practices that enable organizations operating in the digital age to regain control over their technology assets, processes and people.[4]

We hope this report contains the guidance you need to get started creating a more effective technology risk function.

What CIOs are saying

64%

of CIOs say the political, business and economic environment is becoming more unpredictable.

52%

of CIOs are focused on creating a more nimble technology platform to respond to change.

45%

of CIOs are investing in cybersecurity.

32%

of organizations were victims of a major cyber attack in 2017, an increase from each of the past four years.

Source: 2017 CIO survey (KPMG International and Harvey Nash, 2017)

[2] *Changing landscape of disruptive technologies (KPMG International, 2017)*
[3] When we refer to the technology risk function, we mean both the 1st and 2nd lines of defense.
[4] Although the survey results included in this report are consolidated across industries, the survey results from individual industries were consistent in proportion.

Is emerging technology still emerging?

Cloud computing. Connected devices. "Going digital" and "going mobile." Robotics. Blockchain. The fourth industrial revolution has arrived. In fact, these once "emerging" technologies have been around for some time. Adopting them is not an option anymore; it's a mandate to compete in the 21st century.

The velocity of technological change has never been faster than it is now. For enterprises, speed of technology deployment is critical to success and survival, but it can't be at the expense of the health of the organization or its stakeholders and customers.

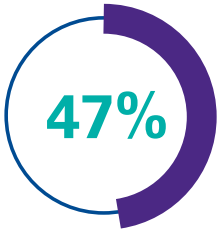
Within the IT departments of many organizations, there has been a strong focus on quickly enabling disruptive technologies so the business can seize its promised benefits—from improved customer experience and increased operational efficiency to boosted profits. However, our data shows that when it comes to technology innovation, many companies struggle to balance the need for speed and agility with the need for control.

KPMG

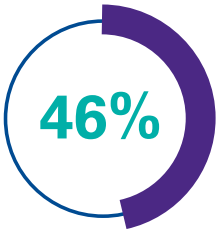
Types of events that would cause an expansion of the scope of technology risk management:*

Half of tech risk executives say emerging technologies within their industries would spur an expansion of their tech risk efforts.

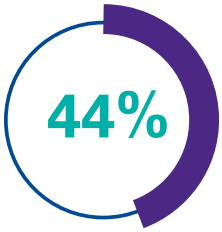
Emerging technologies become prevalent in our organization's industry or beyond.



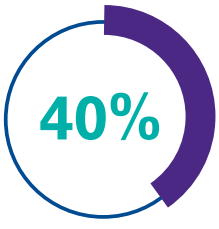
New technologies are identified for potential organizational adoption.



New technologies are deployed within our organization.



Our organization experiences a failure in risk management, control, or compliance.



A regulatory change requires our organization to apply a new lens to IT risk.

"Technology risk management needs to evolve to be prepared for the new world in which disruption is normal. That means IT risk leaders must stop staring down at the steering wheel and look up at where the organization is driving."

—Phil Lageschulte, Partner, KPMG LLP

*Respondents could select multiple responses.

Agile technology risk

The future tech risk professional will need to demystify the risks of new emerging technology and develop an agile tech risk framework with enough flexibility to respond to new risks. An agile technology risk framework will include a dynamic risk assessment that combines the risk appetite of the organization with adoption of new technologies.

Some companies are taking steps to follow through on this promise. For example, we see clients leveraging data analytics and continuous monitoring to change the way they manage technology risk.

But a startling number of organizations aren't walking the talk, as illustrated by the following data.

The reason may be that only a handful of organizations have their arms around such technology and know-how to identify and manage associated risks. But this is the technology risk function's role.

Of course, technology innovation and control should go hand-in-hand. After all, when the risks related to new technologies are expertly managed, organizations can feel much more confident about unleashing them at scale.

Technologies companies are rapidly adopting without assessing the associated risks:*

47% Mobile applications and devices

46% Internet of Things

44% Cloud computing

34% Artificial intelligence

32% Robotics process automation

25% Cognitive computing

14% Blockchain

11% 3D printing

*Respondents could select multiple responses.

KPMG

How do organizations undergoing digital transformation strike the careful balance between innovation and control?

It starts with involving technology risk in strategic planning, investment and business enablement efforts from the get-go. The IT risk function should connect with and understand the larger business strategy and focus on embedding some basic risk management up front in technology adoption efforts, rather than at the back end.

In our experience, success in embedding IT risk into the front-end strategy of technology change often boils down to a number of key factors:

1 The leadership culture at the top of the technology organization.

How do technology leaders embrace, support and drive a culture of risk management? Where is technology risk positioned? Who does it report to? How credible is it? How well funded is it?

2 Where tech risk sits in the organization and who they collaborate with.

Technology risk should collaborate closely with strategic planning teams, including business planning, innovation and technology enablement teams. Read more about technology risk's role and position in the organization in the following section of our report.

3 Willingness of tech risk leaders to change their view from "It shouldn't be done," to "How can it be done with less risk?"

Some technology risk teams are very rigid about the risks associated with emerging technology, and therefore marginalized or kept at arm's length from the strategic planning process. They more often than not hinder the innovation process through resistance and negativity. Rather, they must help enable and support the business growth.

4 The right talent.

While the skills gap is an issue in technology risk—and we discuss it in detail later in this report—the talent issue is more about awareness than capabilities. IT risk officers should educate themselves and the technical risk professionals on their teams about macro business issues, so the technology risk function has the knowledge and understanding it needs to effectively incorporate risk insights into strategic discussions and decisions.

Getting technology risk a seat at the table

With technology increasingly touching nearly every aspect of the business, more C-suite leaders now acknowledge the direct connection between IT risk and enterprise risk—and more broadly enterprise strategy. As such, many organizations are beginning to view technology risk as a value center that helps meet critical business objectives, and are investing accordingly.

"When it comes to technology, risk is always a potential. That potential may erupt, causing a regulatory, customer or safety issue that might have huge financial or reputational consequences. Or it may never manifest into an actual event. If risk management is not embedded up front, companies are rolling the dice. It's like buying an insurance policy that you might never end up using, but if you have to, you'll be very thankful you bought it."

– Phil Lageschulte, Partner, KPMG LLP

KPMG

The technology risk journey from cost center to value creator is well underway...

Technology risk is perceived as helping to meet business needs.

88%

of tech risk leaders believe technology risk is driving value for the organization.

Technology risk and business collaboration is trending up.

82%

of tech risk leaders report proactive communication between functions.

As a result, spending on technology risk is set to accelerate.

49%

of tech risk leaders say tech risk spending will increase over the next three years.

...enabling tech risk activities that are more informed, proactive and trusted.

Beyond compliance

Despite the rising profile of the tech risk function, our survey results indicate that the business and tech risk still do not engage actively enough to manage risks proactively. The tech risk function can maximize impact only when included at the outset of project initiatives.

Although technology risk teams clearly have a larger role to play, their ability to do so is hindered by the fact that an overwhelming majority (87%) of organizations do not currently view IT risk's role as the proactive management of technology risk across the organization.

According to our survey data, organizations primarily view technology risk as an arm of compliance or cybersecurity, rather than an organization-wide function for proactive risk management.

Tech risk seen as reactive and siloed

87%

Tech risk seen as an arm of compliance*

64%

Tech risk seen as an arm of cybersecurity*

37%

*Respondents could select multiple responses.

KPMG

We also found that often, technology risk teams are only included in projects after the fact, once issues begin to arise. At this stage, the impact they are able to make is minimal.

Tech risk teams brought into projects after the fact, only once issues begin to arise

72%

As a result, the business is exposed to more risk.

Beyond compliance (continued)

Other KPMG research backs up the fact that technology risk has a larger role to play when it comes to protecting the organization from risk—especially with regard to cybersecurity.

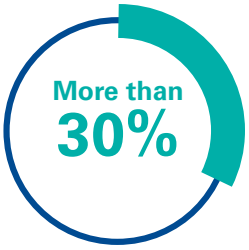
According to KPMG's 2017 U.S. CEO Outlook survey, only **40%** of CEOs say their organizations are well prepared for a cyber event.[5]

In addition, KPMG found that a significant portion of technology incidents are preventable with the right precautions (see sidebar on technology risk's role in preventing blockchain breaches).

In our recent report, *Technology risk radar*, we found that more than **30%** of the 700+ technology incidents we examined over the past year across industries were caused by software glitches.

By engaging technology risk from the get-go, exercising rigor when testing systems, and building the right level of resilience to enable failover, most of the incidents would have been avoidable.[6]

of companies are well prepared for cyber event.



of incidents caused by software glitches.

Blockchain breaches are more preventable with robust tech risk.

Be it legacy systems or new technologies, one of the main underlying root causes of most technology failures is the same: Not including technology risk in early, high-level strategic conversations. KPMG recently studied two recent cyber incidents related to blockchain technology and learned that vulnerabilities and design flaws could have been identified and fixed prior to the breaches, if the impacted companies had engaged tech risk professionals to conduct thorough, formal, end-to-end security reviews.

[5]2017 U.S. CEO Outlook survey (KPMG LLP, 2017)

[6]*Technology risk radar third edition* (KPMG Intanal, 2017)

Source: *Securing the chain* (KPMG International, 2017)

KPMG

How can technology risk gain their warranted seat at the table and increase their impact on the business?

1

For one, technology risk leaders should establish a plan of activity and menu of services that line up with the day-to-day and project-based activities of the IT group that directly support the overall business. For example, technology risk could align its activities with the priority projects in IT's annual budget cycle, even becoming a direct work stream of those projects.

2

It is also important for technology risk to participate in committees and focus groups that are looking at new products or services, with a focus on providing clarity on the potential risks of innovation and strategies to remove obstacles associated with those risks.

3

In addition, top-level tech risk professionals should interact regularly with the CIO, CISO, CRO and COO. Annually, technology risk should also report to the board's risk committee.

Of course, in status meetings and other touchpoints with IT and operational leadership, the heads of technology risk should be very clear about what value the function brings and what authority they have in those discussions—it can't be a "fly-on-the-wall" situation.

In fact, in conversations with business leadership, technology risk leaders should take on the role of friendly "challenger"—using their risk perspective to help think through business issues and question decisions that might increase the organization's risk profile, whether it's the introduction of a new technology or entry into a new market. To be effective challengers, tech risk professionals need broad knowledge of business strategy and processes, as well as the experience and gravitas to speak up with confidence. That will require technology risk to close the skills gap and leverage data more effectively, both of which we discuss later in the report.

4

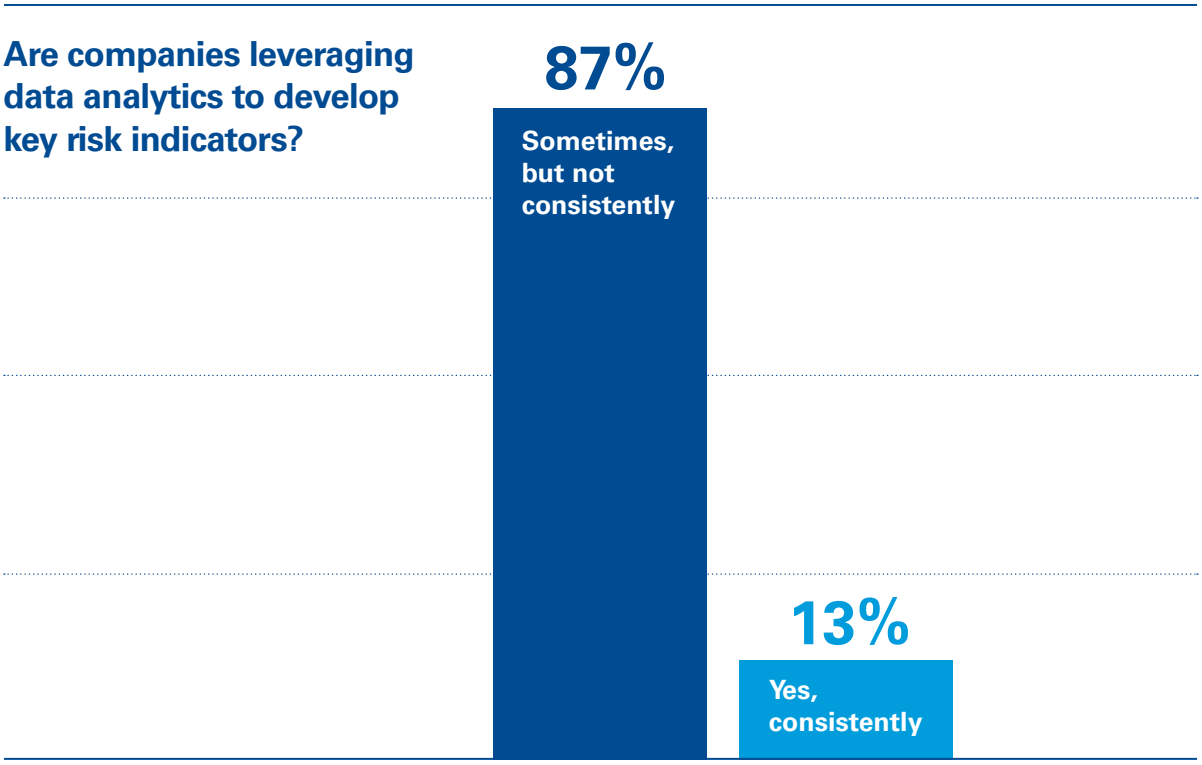
Finally, only establishing a clear tone at the top will make the business want to actively collaborate with technology risk. That requires a dual effort by both technology risk and business leadership. They must work together to show the entire organization that technology risk deserves to be a critical part of the strategic decision-making process, be it about M&A, embracing a new technology, or any business transformation initiative.

"To elevate technology risk, the function must have broader understanding of organizational goals of the technology strategy and serve as a risk advisor. Skill set and capability are critical. When technology risk has the right people asking the right questions, the business and technology stakeholders will naturally come to it."

–Kiran Nagaraj,
Managing Director,
KPMG LLP

Busting the myth around metrics

Organizations define the IT risk universe as all of the tech risks that could potentially impact the business. It's usually a vast number. To understand and manage these risks, the majority of organizations surveyed (92%) use key risk indicators (KRIs)—metrics for measuring the likelihood individual risk events will harm the organization.



KPMG

Meaningful metrics

Although clients are increasingly aware of the concept and value of KRIs, and adoption and implementation of KRIs is widespread in some sectors, KRIs don't always match up well to the actual technology risks facing the organization.

The risks aren't obvious.

Sometimes, the risks aren't obvious. There could be numerous reasons businesses lack full transparency into the scope of technology risks that might affect them.

KRIs are only viewed individually.

Perhaps KRIs are only viewed individually, rather than collectively. Viewing KRIs together rather than individually often leads to a deeper understanding of the risk and a stronger call to action. However, many organizations are struggling to rationalize and consolidate numerous enterprise systems across technology and operational functions. When there is no single, golden source of data, it's hard to get a good handle on what data you have, let alone classify it, categorize it and make sense of it.

KRIs emerge from unfamiliar parts of the business.

KRIs may emerge from parts of the business that aren't traditionally familiar to the technology risk function. For example, organizations may be overly focused on compliance and controls rather than risk management, so they fail to define KRIs for risks that fall outside the scope of those areas, such as audit, regulatory and compliance. As such, emerging risks, such as those associated with cybersecurity, automation, cloud computing, or artificial intelligence, might be overlooked.

Poor data quality.

Data quality can also impact the effectiveness of KRIs. If the KRIs are based on poor quality data, business leaders may hesitate to take action based on those KRIs.

"Limitations on leveraging KRIs in the IT risk space include:

- **A focus on compliance and controls rather than risk management**
- **Pressure against investing in IT risk beyond the minimum baseline activity**
- **Unreliable data sources, data and risk correlation**
- **Difficulty in determining risk measurement criteria and the subjectivity of those criteria**
- **Lack of confidence in actions taken based on KRI measurements**
- **Lack of clarity on whom to escalate KRI results for final authorization of action."**

–Joshua Galvan, Principal, KPMG LLP

Using KRIs

How can organizations use KRIs more effectively to assess the organization's true technology risks?

We have found that effective KRIs have the following characteristics:

— **A smaller set of metrics** is generally easier to maintain, monitor and manage.

— **They serve as a measure of risk.** Their definitions are agreed upon by key risk stakeholders to serve as a measure of risk, rather than a one-off issue, bug or event.

— **They have underlying supporting data,** usually housed in a data dictionary, which includes a metric formula, data elements and risk taxonomy which enables technology risk to map and track risks from business unit to enterprise level.

— **They are measurable and actionable**. They tie directly to the business impact, enabling technology risk to speak to the business in meaningful and attention-grabbing terms, such as lost dollars or customers.

— **They are regularly maintained, monitored and refreshed.** When a metric fluctuates, someone pays attention, makes a decision and takes action.

"With the increasing impact of emerging technology in most industries, speed and velocity of the risk are now absolutely necessary criteria in the technology risk management formula."

–Vivek Mehta, Partner, KPMG LLP

KPMG

Best practices for technology risk to overcome the challenges of leveraging KRIs:

Develop an organization-wide risk mind set.

When IT risk is top of mind across the organization, it helps technology risk build confidence in and support KRI development. There are many creative ways to develop an organization-wide risk mind set, such as by rewarding risk management activity, especially in technology solution development and delivery teams.

Embed risk remediation tools and practices across IT.

Many business leaders think that each time they identify a risk, they need to start over on how to remediate it. In reality, there may be good practices that already exist in the environment.

Leverage existing risk measurement capabilities.

Non technology risk functions, such as IT operations, have their own, predefined KRIs that the business is already familiar with. If technology risk adopts those KRIs, it can reduce ramp-up and buy-in time.

Link risk identification to strategic business objectives.

To appropriately identify and assess the organization's true technology risks, tech risk professionals need to proactively engage and integrate with business units. Not only does this enable technology risk to bring more value, but it helps organizations avoid duplicate efforts with other teams, such as enterprise risk management.

Predictive KRIs

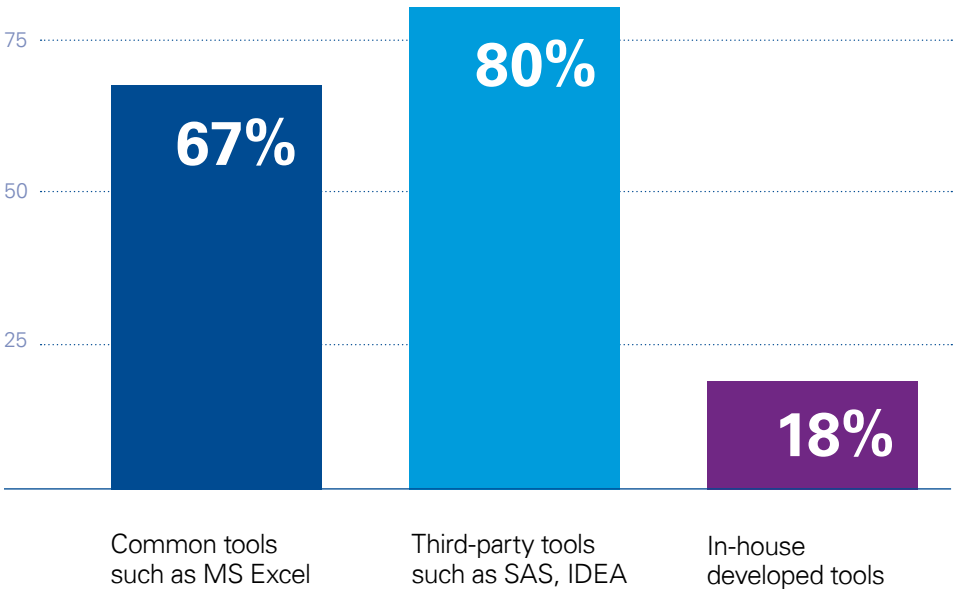
In all of this talk about risk metrics, we have not yet mentioned what is perhaps the most important kind: predictive KRIs. Data on technology risks can be employed to establish patterns that can help predict potential issues before they happen. And predictive KRIs are ideal for proactively managing technology risks. But only 13% of companies surveyed consistently leverage predictive risk indicators.

13% consistently leverage predictive risk indicators

More organizations haven't embraced predictive KRIs in part due to feasibility and practicality issues. Resource challenges play a role. While predictive KRIs may be valued, they may not be fully bought into by the business stakeholders who prefer to use resources elsewhere, thereby inhibiting true risk management. For example, if the KRI indicates a need to refocus people, systems or dollars to preempt an issue, it can come as a sacrifice to other operational, compliance, and risk management priorities.

Survey results also indicate that most organizations use third-party tools such as SAS and IDEA to develop predictive risk indicators. However, it is unclear whether they are using the tools' outputs in their risk reports or for proactive risk management.

Many organizations are still using common tools, such as MS Excel, to develop key risk indicators or KRIs:*



*Respondents could select multiple responses.

KPMG

"To enhance their ability to predict technology risk, companies should invest in analytics and cognitive capabilities, effective dashboard reporting, and improved data reliability and access."

–Joshua Galvan, Principal, KPMG LLP

*Respondents could select multiple responses.

Talent trials

Across industries, technology risk's biggest challenge is the skills gap, according to our survey data. This echoes a problem common to all of IT. In each of the last four years, 60% of respondents to the KPMG International and Harvey Nash CIO survey reported skills shortages, with big data/ analytics topping the list of most in-demand skills.[7]

The skills gap is driving many of the challenges in demonstrating technology risk's ability to add value.

New skill sets

As mentioned earlier, for tech risk professionals to truly add value, they must participate in front-end strategy discussions, especially as new disruptive technologies enter the organization. Tech risk professionals need to actively stay in front of what's happening in the business regarding disruptive technologies, putting the risk lens on them before they are adopted. At the same time, many technology risk functions are looking to become leaner and more collaborative with other risk teams to reduce redundancy and process inefficiency, especially with respect to risk and compliance assessments and reporting.

Both these realities require a new set of fundamental skills. Today's tech risk professionals, at every level, need:

- Business understanding
- Technology understanding
- Risk management and controls understanding
- The ability to make sense of risk data from a business context.

[7]2017 CIO survey (KPMG International and Harvey Nash, 2017)

KPMG

"It's hard to build skills to manage the risks of a new, unknown technology that's not here yet. There's a bit of runway—a year or two—before the technology even reaches a pilot phase in a big enterprise. That runway—when the business is deciding whether or not to invest in or adopt a particular technology—is what technology risk should use to understand what that technology truly represents for their group from a talent perspective."

—Kiran Nagaraj,
Managing Director, KPMG LLP

How should technology risk transform the workforce to meet tomorrow's demands?

Some organizations are focused on training tech risk professionals with the business knowledge and mind set necessary to contribute to important, high-level discussions on enterprise risk. But training is just one part of it. For the business to truly accept and respect the technology risk function, other changes are likely necessary, such as higher compensation and pay grades to tech risk professionals, physical location near key business stakeholders, and more regular inclusion in board and management meetings.

Digital labor

Technology risk functions are also challenged by the secondary impacts of automation on the workforce and the business. Some organizations are recognizing that big data, automation, cognitive, and artificial intelligence tools can be accelerators for technology risk—they can even overcome the skills gap through better data and solutions.

But while the rapid adoption of cutting-edge technologies brings a host of cost savings and business model enhancements, such business transformation initiatives can lead to significant risk without equal attention being paid to labor force impacts, societal implications and alignment with an organization's core values.[8]

How should technology risk functions manage the impact of automation on the workforce?

In light of the changing workforce landscape, trends indicate that many organizations are shifting from consumers of work to builders of talent, focusing on creating resilient, long-term career opportunities for employees.

"Organizations don't need 1,000 people doing reconciliations if they have a system that does reconciliations with just 10 people overseeing it. That's the potential of automation, AI and cognitive."

—David DiCristofaro, Partner, KPMG LLP

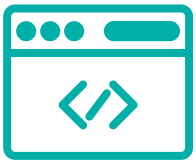
[8] *An ethical compass in the automation age* (KPMG LLP, 2017)

KPMG

CEOs surveyed for KPMG's 2017 U.S. CEO Outlook survey say their organizations are increasing investment in the following areas:[9]

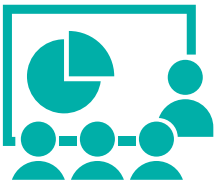
Recruitment

80%



Digital infrastructure

58%



Workforce training

57%

[9]2017 U.S. CEO Outlook survey (KPMG LLP, 2017)

Rethinking risk data and reporting

Although more than 80% of tech risk executives surveyed report that their organization's key stakeholders have confidence in their data, discussions with senior industry leaders and clients—as well as other KPMG research—tell us otherwise.

Data integrity

The results from this survey show:

Technology risk execs

Confident 82%

82% of tech risk executives report that key stakeholders have high confidence in their risk data.

However, according to KPMG's recent CEO Outlook survey:

CEOs

Concerned 49%

Almost half of CEOs question the integrity of the data they base their decisions upon.[10]

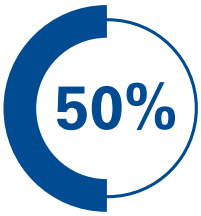
[10]2017 U.S. CEO Outlook survey (KPMG LLP, 2017)

KPMG

Data collection methods

Our survey results show that half of companies have not formalized their data collection process. Most of the data gathering for risk reports is still done through ad hoc/informal means.

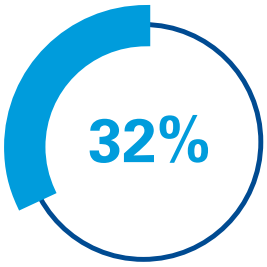
Informal process



Ad hoc inquiries

Informal activities where IT risk data is collected through conversations, anecdotes, etc.

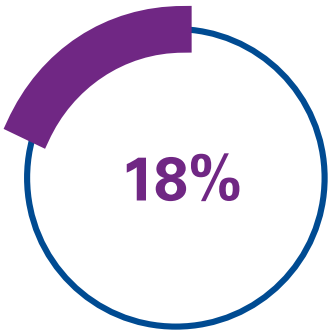
Formal process



Periodic risk assessments

Formally-timed activities where IT risk data is collected through a standard process and rigorous techniques

Automated process



Live risk register data

Automated capability where IT risk data is collected through system-based sources

This least-used data collection methodology provides the most proactive risk mitigation.

"Too many organizations are going for volume vs. quality of data. While a lot of blame for tech risk issues is placed on the data, the real challenge is lack of consistency about what data should be used and how—for example, applying the right filters and criteria. Tech risk must get better at filtering and parsing through data in a meaningful, consistent way so it can effectively communicate how data links to business impact."

–Vivek Mehta,
Partner, KPMG LLP

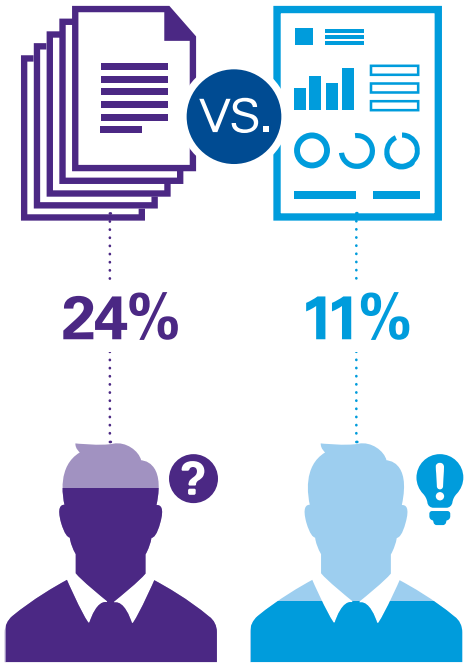
"Most risk data is being produced with what is available without having started with what's necessary to know for decision making. It is way too detailed and it completely misses the 'so what?' It produces more shock value than true value."

—Robert Westbrook, Principal, KPMG LLP

Turning data into insights

Many technology risk leaders are clearly making a strong effort to keep senior business leaders informed. The survey data shows that:

C-level executives are more likely to receive detailed reports than dashboards with high-level insights.



Details are great, but it is also critical that risk reporting to senior management is understandable, actionable, and impactful.

One common problem technology risk functions encounter in reporting their data is its scope, which can make it difficult to extract meaningful insights from it. Report detail should be commensurate with the audience type and level. But often, reports do not effectively link the risk data and the organization's risk appetite.

In addition, it currently takes too long to create risk reports, especially when data is gathered from ad hoc mechanisms as opposed to systems of record and it isn't normalized. By the time the leaders get them, the true impact is diminished and the goalposts are moved.

Too much volume with too little analyses delivered too slowly often leads to a "white noise" problem.

When volumes and volumes of granular data are not being synthesized at an executive level and translated into what the true business impact is—in a timely fashion—it is difficult for stakeholders to make sense of, let alone act on, the information they consume. As a result, senior leaders and boards tend to pendulum-swing from panicking to ignoring the data.

Many technology risk leaders find they need to simplify the issues and the conversation, and learn to speak the same language as business stakeholders.

KPMG

Tech risk functions can address risk data and reporting challenges in a variety of ways.

1 Establish clear standards

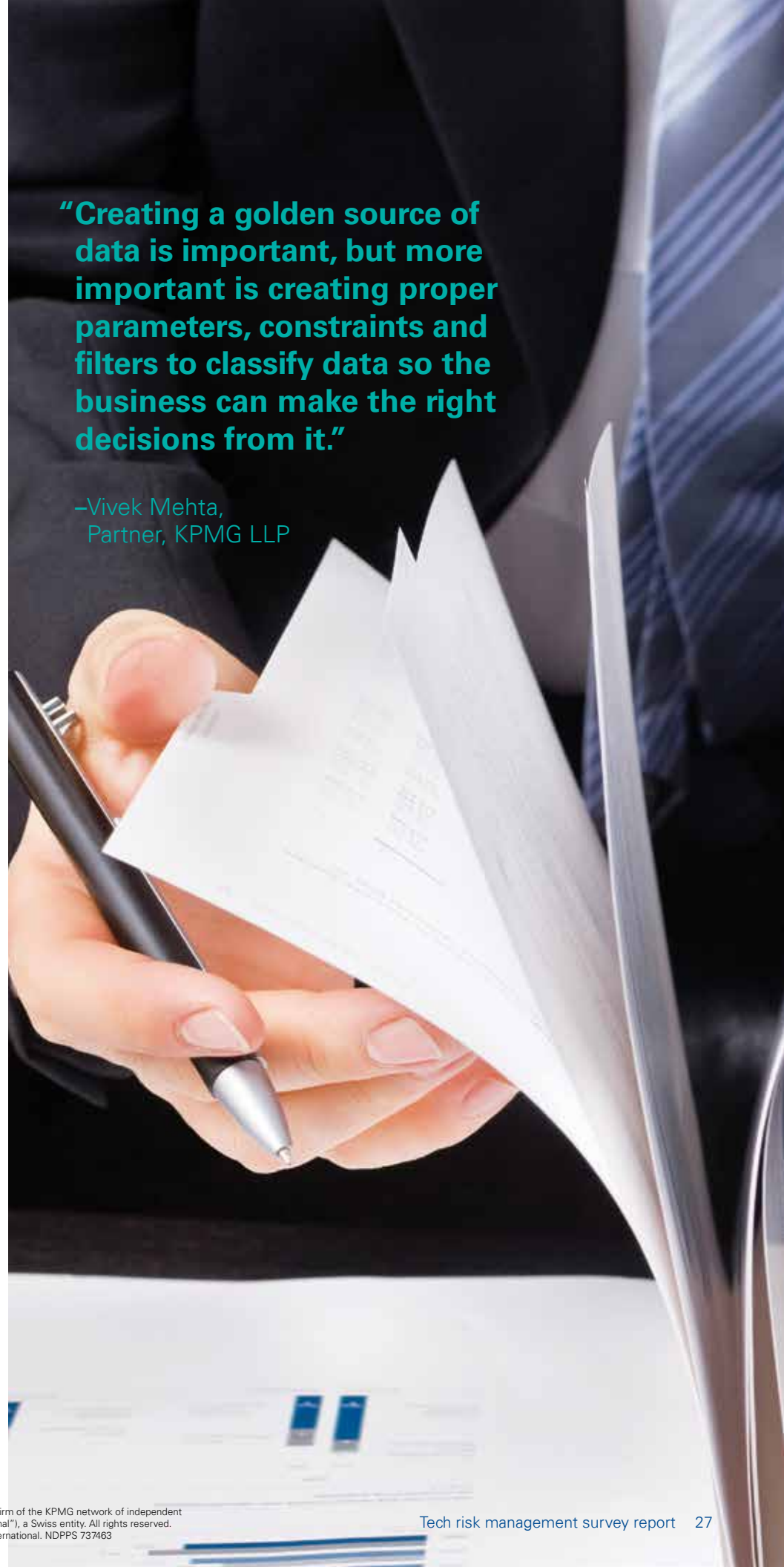
First, technology risk should establish clear standards around risk reporting and risk data, such as a data dictionary that defines data sources and uses. It is also critical to establish strong data governance processes to ensure data is classified and stored correctly, owned by the appropriate group, and checked and tested for quality.

2 Create personalized dashboards

Second, to communicate more effectively with the business, technology risk groups need to create personalized reporting dashboards and formats for different audiences, containing the appropriate level of detail for each one. Digital and mobile applications that allow business leaders to both visualize and drill down into data with ease, offer the potential to replace conventional risk reports, while also helping technology risk become much faster at reporting changes in risk data.

3 Provide qualitative insights

Third, it's also important to remember that qualitative insights will always have a place in IT risk management. Business decisions aren't usually driven only from a risk score, but rather collectively by everything technology risk does.



"Creating a golden source of data is important, but more important is creating proper parameters, constraints and filters to classify data so the business can make the right decisions from it."

–Vivek Mehta,
Partner, KPMG LLP

Final thoughts: Creating next-generation technology risk management

As technology becomes increasingly complex, open and ubiquitous, both business and IT executives are becoming more sensitive to technology risk. They are also becoming more cautious and risk-savvy. In this environment, technology risk has a lot to contribute.

Next-generation technology risk functions will understand the business better, predict risks associated with new technologies or legacy systems, manage risks proactively, and improve the organization's resiliency should an incident happen. We hope this report helps you get there.

"Technology risk should not be an added cost to doing business with no value added. If there is a way for technology risk to be a money maker for the business—such as if companies can glean insights from firm, customer or supplier behavior gathered during the process of doing technology risk—that would be gold."

—Constance Hunter, Principal, KPMG LLP

KPMG

Next-generation tech risk functions will have:

Contributions to strategy discussions	As the pace and complexity of technology increases—and increases the organization's risk profile—leading-edge organizations will integrate risk management from the get-go, preparing and managing risks in line with the business strategy.
Strong business acumen	Tomorrow's best tech risk professionals will have the business knowledge to translate risk and its impact into comprehensible language for decision-makers. They'll have both the understanding and the visibility to find the ideal middle ground, where risk is mitigated upfront but business growth is still enabled.
A seat at the business table, including more collaboration with business stakeholders	Leading-edge organizations will find religion and move technology risk more toward the business.
An increase in brand recognition within the organization	Leading-edge organizations will elevate technology risk's profile within the organization and view it as "more than just compliance."
A budget and headcount commensurate with the business and technology budget and headcount	Leading-edge organizations will move away from measuring IT risk management spending solely as a percentage of compliance.
Nimble data models	Rather than focusing on increasing the overall volume of risk data and metrics or the number of risk categories metrics cover, leading-edge organizations will emphasize trust and agility, perfecting data models that can absorb new risks and define new controls as changes in the external environment impact the organization's risk exposure.
Outcome-focused reporting	Business leaders need meaningful information to make the right decisions. Leading-edge organizations will synthesize risk data at the executive level and tie data directly to business impact.
A key role at all stages of technology adoption, implementation and change	The future tech risk function will demystify the risks of new emerging technology and develop a framework with enough flexibility to respond to new risks. During and after adoption, the team will continuously stress test processes, monitor performance, track metrics and report to management.

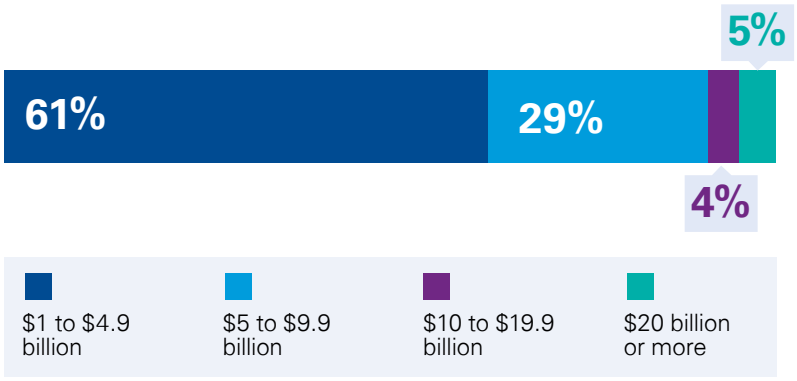
Survey methodology and demographics

In April 2017, KPMG—in collaboration with Forbes Insights—conducted a telephone survey of senior executives responsible for IT risk management (technology risk) at large U.S. enterprises.

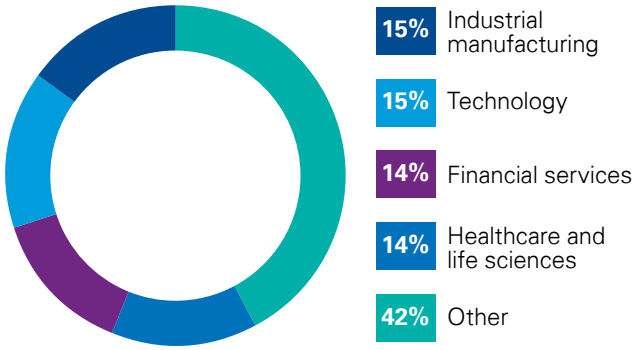
We first developed a set of questions across three main themes by engaging our technology risk leadership within the firm. We then worked with Forbes to help field this survey to approximately 200 respondents across four industries—namely, financial services, technology, healthcare and life sciences and industrial manufacturing. We made sure our respondents spanned across the lines of defense.

Based on the responses we received, we analyzed the data and extracted key themes and insights included in this report.

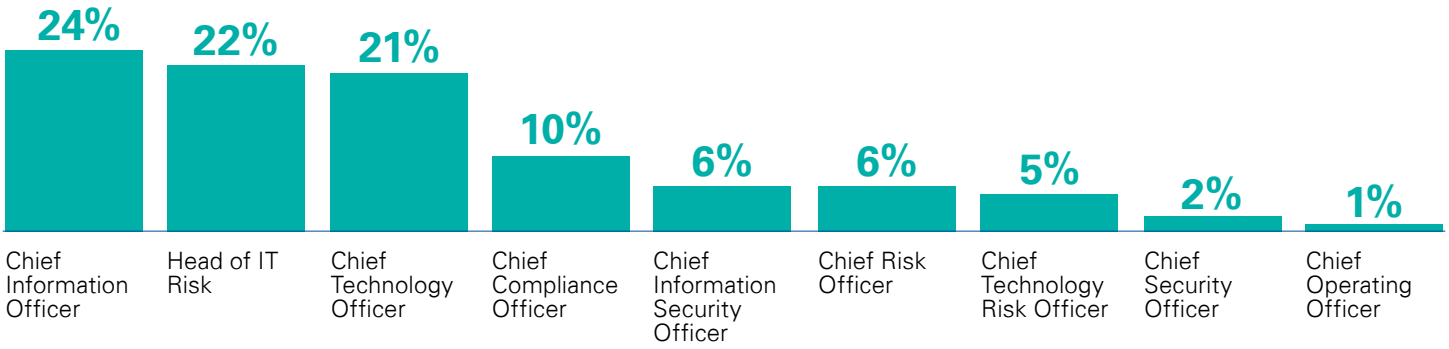
Annual revenue



Industry



Title



KPMG

How KPMG can help

Today more than ever, technology is a critical enabler of the business. We help clients recognize and responsibly manage the complete universe of risks associated with their technology environment, so they can realize the rewards of the digital age. With services backed by industry-leading methodologies and processes, combined with experienced professionals with deep technical and strategic know-how, we have helped numerous organizations transform IT risk management from cost center to value creator.

KPMG

Authors

Phil Lageschulte
Partner, KPMG LLP
Service Line Leader,
Global IT Advisory
pjlageschulte@kpmg.com

Vivek Mehta
Partner, KPMG LLP
Emerging Technology Risk
vivekmehta@kpmg.com

Joshua Galvan
Principal, KPMG LLP
Emerging Technology Risk
jgalvan@kpmg.com

Rob Westbrook
Principal, KPMG LLP
Emerging Technology Risk
rwestbrook@kpmg.com

Kiran Nagaraj
Managing Director, KPMG LLP
Emerging Technology Risk
kirannagaraj@kpmg.com

Priya Mouli
Manager, KPMG LLP
Emerging Technology Risk
pmouli@kpmg.com

Contributors

Thank you to the following contributors for adding their insights to this report.

David DiCristofaro, Partner, KPMG LLP

Constance Hunter, Principal, KPMG LLP

Contact us

Phil Lageschulte
Partner, KPMG LLP
Service Line Leader,
Global IT Advisory
T: 312-665-5380
E: pjlageschulte@kpmg.com

Vivek Mehta
Partner, KPMG LLP
Emerging Technology Risk
T: 212-872-6548
E: vivekmehta@kpmg.com

Charles Jacco
Principal, KPMG LLP
Cyber Security
T: 212-954-1949
E: cjacco@kpmg.com

Priya Mouli
Manager, KPMG LLP
Emerging Technology Risk
T: 408-805-2787
E: pmouli@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/us/riskconsulting