ISACA

CMMI Institute

infosecurity GROUP

STATE OF **ENTERPRISE RISK MANAGEMENT** 2020

ENTERPRISE RISK RESEARCH BRIEF

CONTENTS

ABSTRACT

ISACA®, CMMI Institute® and **Infosecurity Group** surveyed a global population of over 4,500 professionals involved in risk decisions for large and small enterprises, across six continents and all industries, from manufacturing to government and financial services, and every industry in between. The goal of the survey was to provide insight, gain perspective and guide enterprises' risk management programs.

State of Enterprise Risk Mananagement 2020 reports, analyzes and presents the key findings from the survey. This research brief also provides conclusions about risk management practices, and risk management areas of opportunity and guidance for boards of directors and executive teams.

Executive Summary

Enterprise risk management can be challenging. On the one hand, there are natural human instincts that can be difficult to overcome that can interfere with objective and systematic risk analysis and mitigation. For example, practitioners who make risk decisions on behalf of their enterprises (e.g., risk managers, cybersecurity specialists, auditors, and governance and compliance practitioners) can be directed to advocate so strenuously and so often in favor of risk reduction that they can sometimes forget that risk management is about optimizing risk rather than removing it entirely. They may focus on unexpected or unplanned events that may impact profitability, competitiveness or reputation but ignore the fact that failure to incur the right risk can likewise be potentially problematic, by causing enterprises to stagnate, lose competitiveness/market share or otherwise underperform their competition. On the other hand, the importance of assessing, mitigating, managing, measuring and tracking risk is well known; enterprises should assume only appropriate risk and avoid or mitigate excess risk--or potentially incur dire consequences.

Finding the right middle ground is as important as it is challenging. Because the business landscape is constantly shifting, new risk can emerge, allowing relatively little time for enterprises to respond. For example, low-risk applications or business processes can suddenly take on a whole new dimension of risk. This scenario is against a backdrop of attackers and external threat actors who continue to innovate and leverage new technologies to pursue their nefarious intent, geopolitical risk that can cause regional dynamics to shift, financial markets (e.g., historical securities and derivatives markets and the new cryptocurrency market) that can turn suddenly, and increasingly interdependent supply chains that expand logistical complexity. The turbulence in the risk landscape is unprecedented.

With this in mind, it is natural for organizations to ask how they fare relative to other enterprises in their risk efforts. For example, enterprises question if they are too risk averse or not risk averse enough, if they invested the right amount in risk management processes to bring about the correct maturity level to accomplish their goals, and if they implemented the correct steps to ensure optimization.

To help enterprises answer these questions, gain perspective and guide their risk management development, ISACA, CMMI Institute and Infosecurity Group surveyed those who are best equipped to know—a global population of over 4,500 specialists involved in risk decisions for large and small enterprises, across six continents and all industries, from manufacturing to government and financial services, and every industry in between.

State of Enterprise Risk Management 2020 reports, analyzes and presents the key findings from the survey. This research brief also provides conclusions about risk management practices, and risk management areas of opportunity and guidance for boards of directors and executive teams.

Because the business landscape is constantly shifting, new risk can emerge, allowing relatively little time for enterprises to respond.

Key Findings

Following are the key survey findings:

- **Risk areas are generally well understood by businesses, but execution of risk management can be improved significantly.**
- **Cybersecurity risk is an emerging and key challenge area.**
- **Cloud-related risk concerns forecast similar concerns for new and emerging technologies.**
- **Although technology risk is high, traditional risk remains a concern. Specific areas of concern about traditional risk vary by geography and industry.**

In the body of this research brief, we outline the key data points, supporting conclusions, analysis and thought behind these findings.

Survey Methodology

In July 2019, ISACA, CMMI Institute and Infosecurity sent survey invitations via email to a global population of individuals responsible for elements of risk management in their enterprises. These individuals perform risk management roles in:

- Audit/Assurance
- Governance
- Security
- Risk
- Privacy
- Compliance

The survey data were collected anonymously via SurveyMonkey. A total of 4,625 individuals from 140 countries and six continents responded.[1] **Figure 1** shows survey-respondent demographic norms.

It is important to note some characteristics that reflect the survey population's diversity. Among those surveyed, respondents hailed from over 17 industries (**figure 2**).

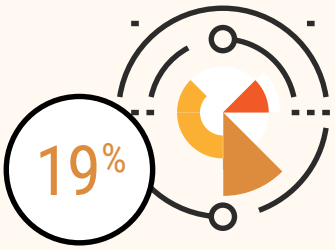
The survey, which used multiple-choice and Likert scale formats to assess enterprise risk management, asked questions about seven major areas:

- Risk awareness
- Perceived risk increase or decrease
- Types of risk
- Risk management methodology employed
- Maturity of risk management practices
- Risk forecasting
- Risk tracking and reporting

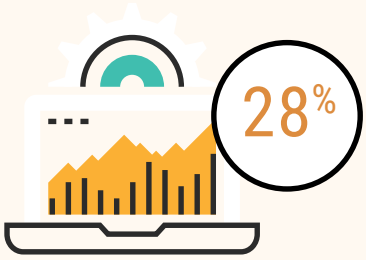
[1] Survey data were collected anonymously online. Certain questions included the option to choose "Don't know" from the list of answers. Where appropriate, "Don't know" responses were removed from the calculation of findings. Result percentages are rounded to the nearest integer.

FIGURE 1—RESPONDENT DEMOGRAPHICS

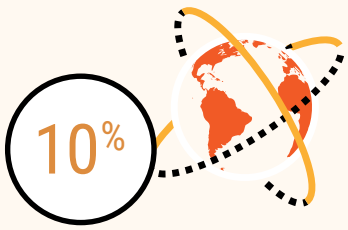
INDUSTRIES



TECHNOLOGY SERVICES/CONSULTING

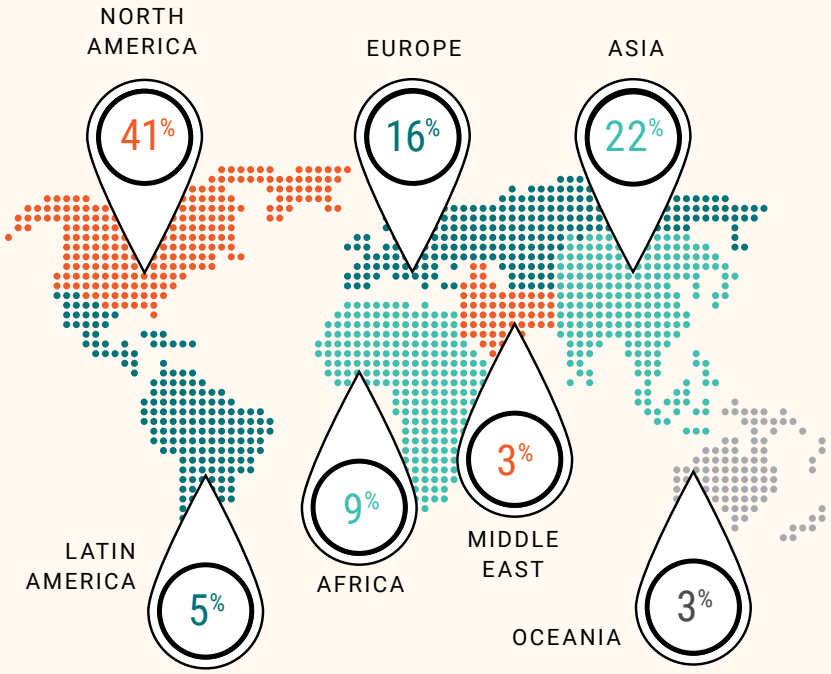


FINANCIAL/BANKING

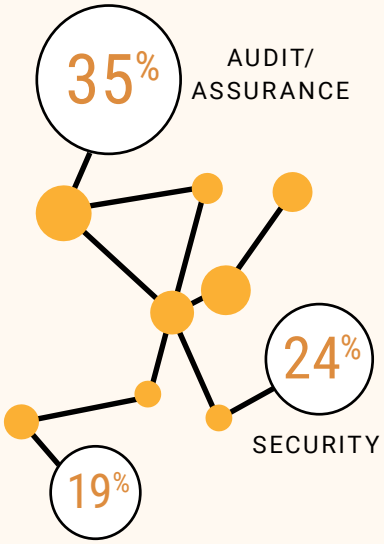


GOVERNMENT/MILITARY—NATIONAL/STATE/LOCAL

REGIONS



MAIN AREA OF RESPONSIBILITY



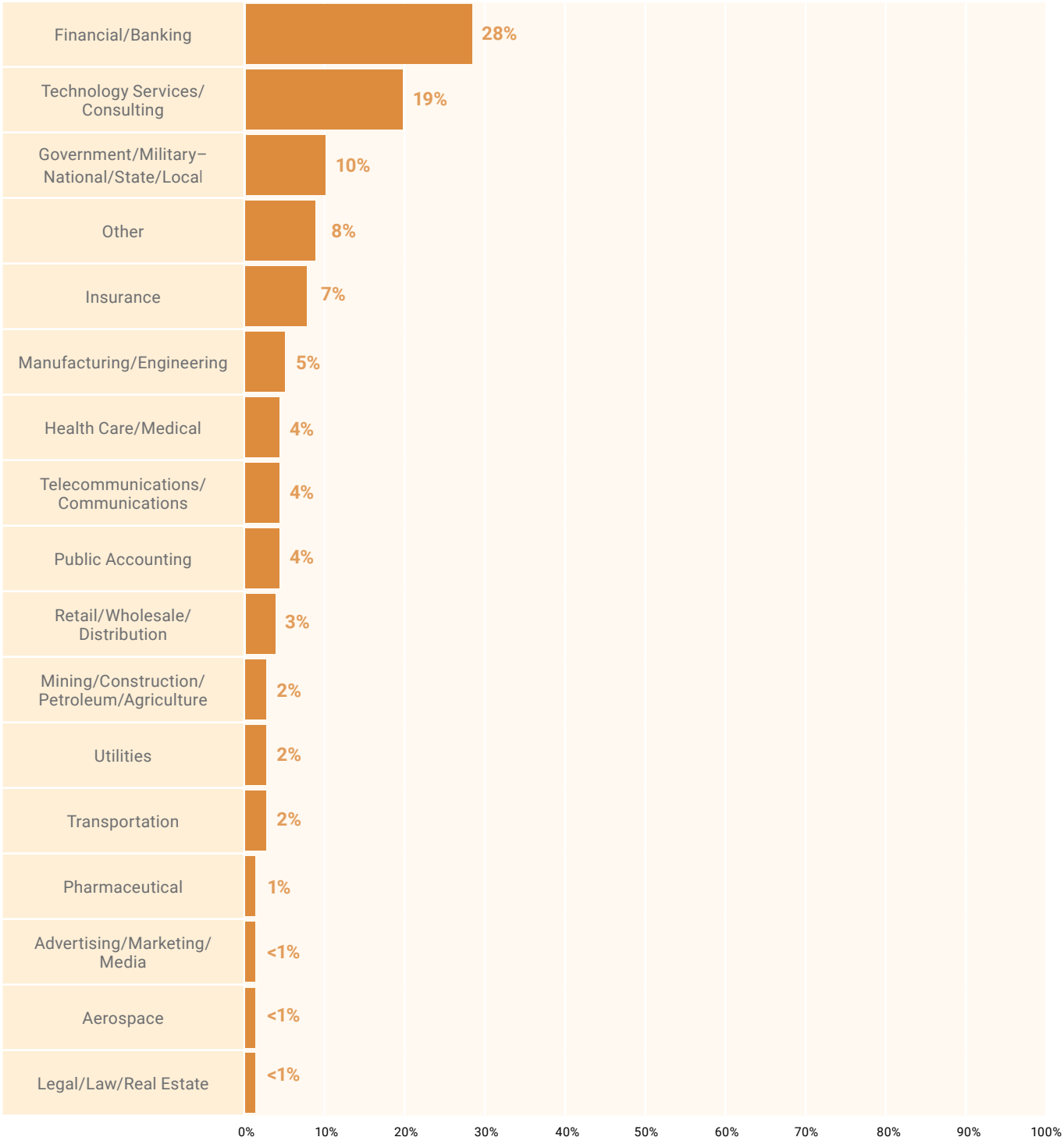
EMPLOYED IN AN ENTERPRISE WITH AT LEAST

1,500

EMPLOYEES

FIGURE 2—INDUSTRY SECTORS

Which of the following, if any, best describes your business category?



Risk Areas Are Well Understood, but Risk Management Can Be Improved Significantly

The survey data show that respondents—particularly those who are at a more senior level in the organizational hierarchy—understand well the most critical risk that challenges their enterprises. They understand both what the risk is—as well as the consequences—should undesirable outcomes occur. Sixty-seven percent of those surveyed indicate that they are either extremely or very familiar with the current business and technology risk facing their enterprise.

What is interesting is that risk awareness correlates to seniority. As the respondent seniority level increases, the more aware they are of the risk that their enterprise faces. Eighty-six percent of respondents at an executive-level job, 80 percent of respondents at a director-level job, 66 percent of respondents at a manager-level job and 55 percent of respondents at a staff-level job are either extremely or very familiar with the business and technology risk (**figure 3**).

This is positive news, because a lack of appropriate understanding of risk can be a barrier to ensuring that an enterprise takes appropriate action to address that risk. Because decision makers with more organizational authority understand the risk better than others (at least in aggregate), enterprises may be able to translate that understanding into appropriate actions to address risk.

Survey respondents report that all risk increased over the past 12 months. Fifty-three percent of those surveyed reported that risk has increased generally (**figure 4**), although it is noteworthy that there is some difference in perception of increased risk based on geography. Respondents from Asia, Oceania and Africa cite overall risk increases to a greater degree than other global regions—this observation is particularly striking in Africa (**figure 5**).

FIGURE 3—RISK AWARENESS BY SENIORITY LEVEL
How familiar are you with both the business and technology risk faced by your organization?

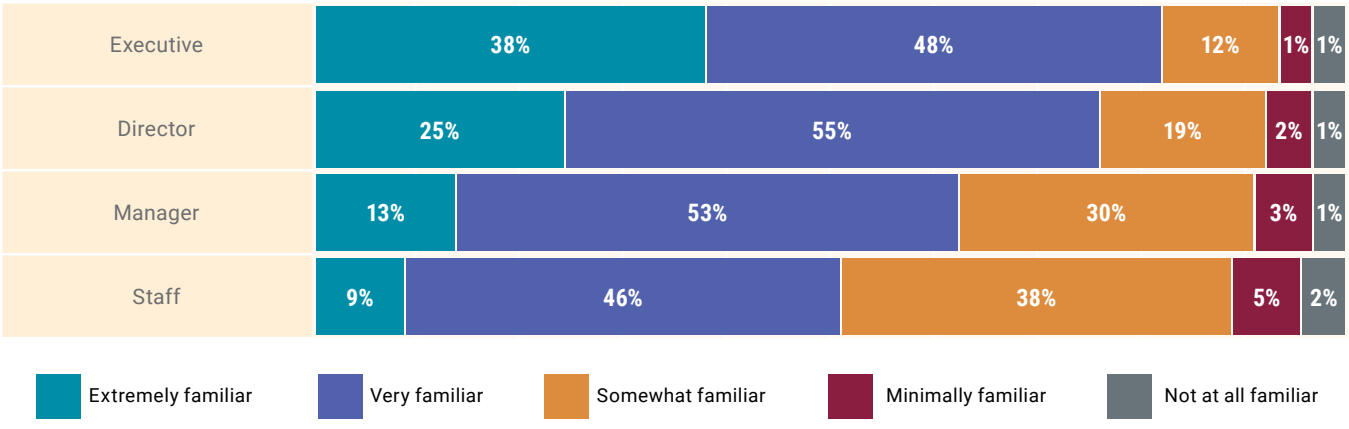


FIGURE 4—CHANGE IN OVERALL RISK AMOUNT COMPARED TO 12 MONTHS AGO

In comparing your organization's overall risk (all types of risk to the business) to 12 months ago, has your organization's risk:

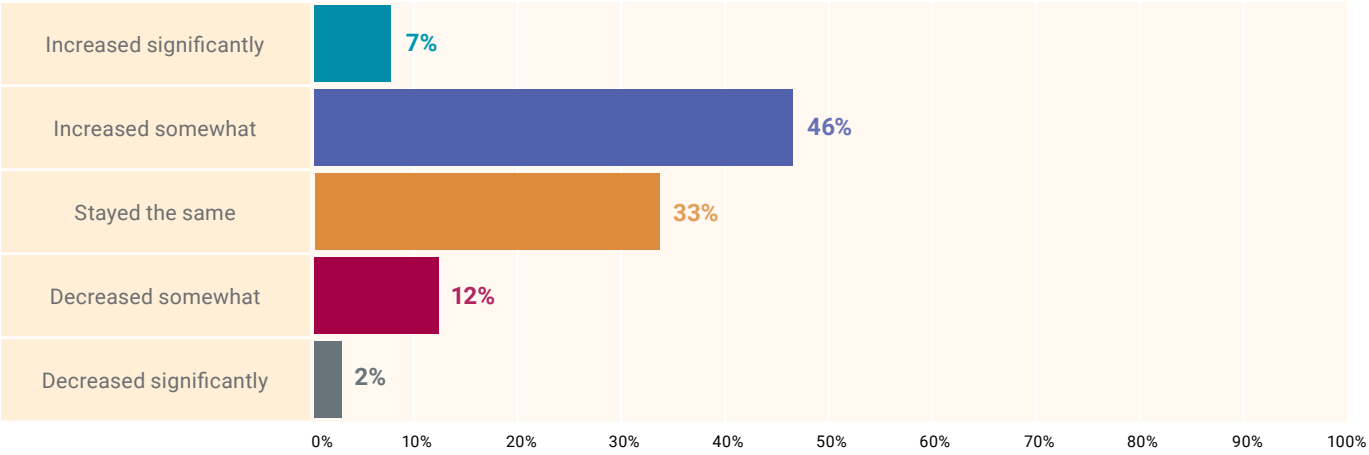
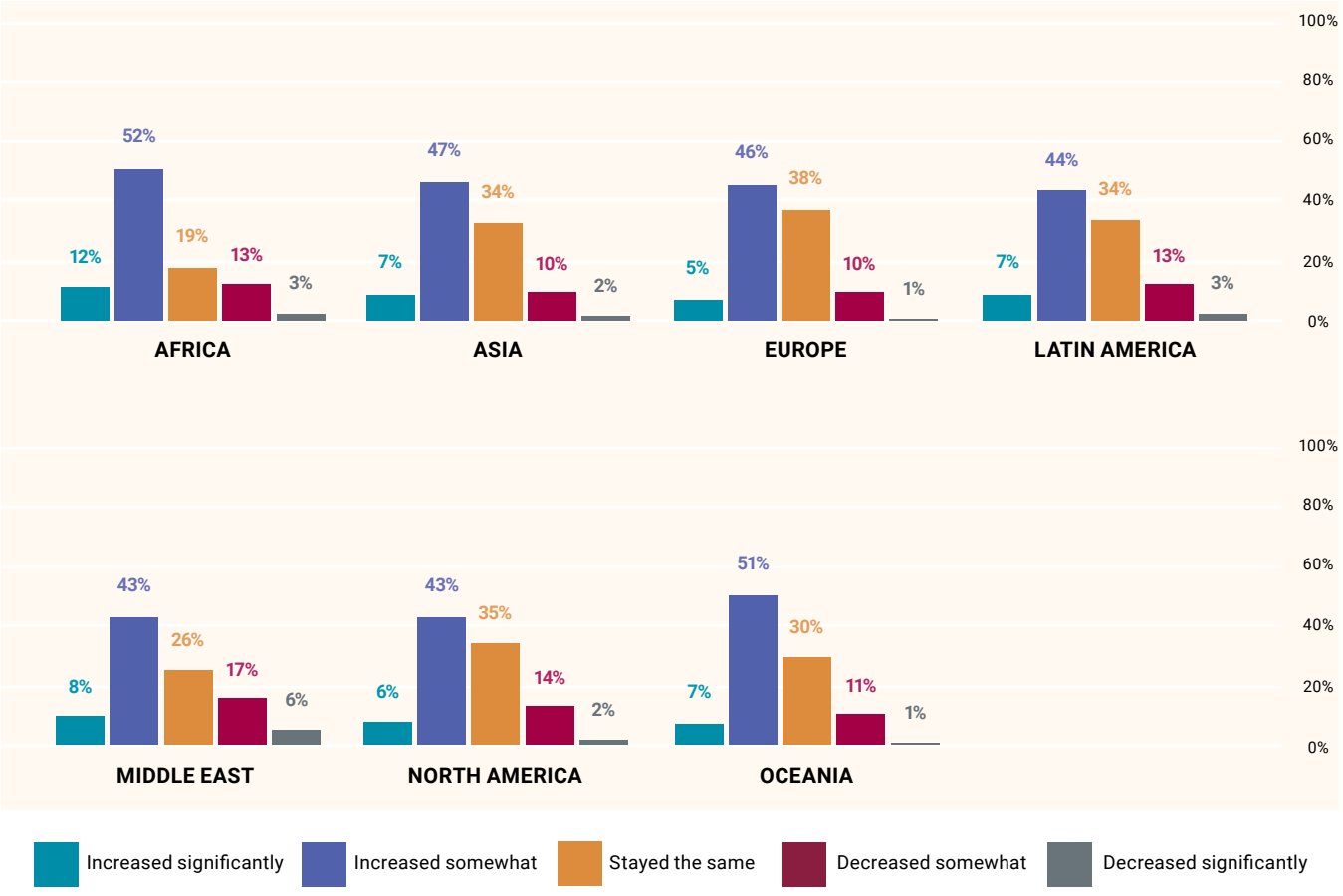


FIGURE 5—CHANGE IN OVERALL RISK AMOUNT COMPARED TO 12 MONTHS AGO BY GLOBAL REGION

In comparing your organization's overall risk (all types of risk to the business) to 12 months ago, has your organization's risk:



The more concerning news relates to the implementation of risk management practices in enterprises. Despite awareness of risk, how enterprises manage risk can be improved. This is true from a maturity and an efficacy standpoint. Although most survey respondents indicate that their enterprises have implemented the most fundamental risk management steps, including assessment (85 percent) and risk identification (81 percent), ongoing measurement and tracking of risk is less developed, and the ability to forecast new risk presents an area of challenge (**figure 6**).

Risk Management Maturity

Although over 80 percent of respondent enterprises undertake basic risk management steps, the maturity of the risk management process is, on the whole, less than expected given the relatively high adoption of these steps. Only 38 percent of respondents indicate that their enterprises have processes at either the managed or optimized level of the maturity spectrum for risk identification, which is one of the highest adopted risk management steps. Only 63 percent of respondents report having defined processes for risk identification. Results for risk assessment maturity were similar—42 percent at the managed or optimized level and 64 percent having defined processes. These were the highest maturity levels for all risk assessment phases reported (**figure 7**).

Although more than half of respondents indicate that their enterprises are in the upper portion of the maturity spectrum (i.e., defined or higher), it is noteworthy that enterprises realize that risk is increasing and have a high degree of awareness for the risk that their enterprises face, but they do not have a higher maturity of risk management processes in place. These results show the opportunity for improvement in the way that enterprises assess, track and manage their risk overall and a global need for improvement of risk management maturity.

Part of the underlying dynamic for these needs may be the enterprise challenges in establishing well-defined risk tolerances. When asked about cybersecurity risk tolerances, only 35 percent of respondents report that their enterprise has a defined (either completely defined or very defined) view of the risk tolerances for their organization.

FIGURE 6—EMPLOYED RISK MANAGEMENT STEPS

Which, if any, of the following risk management steps does your organization employ? Select all that apply.

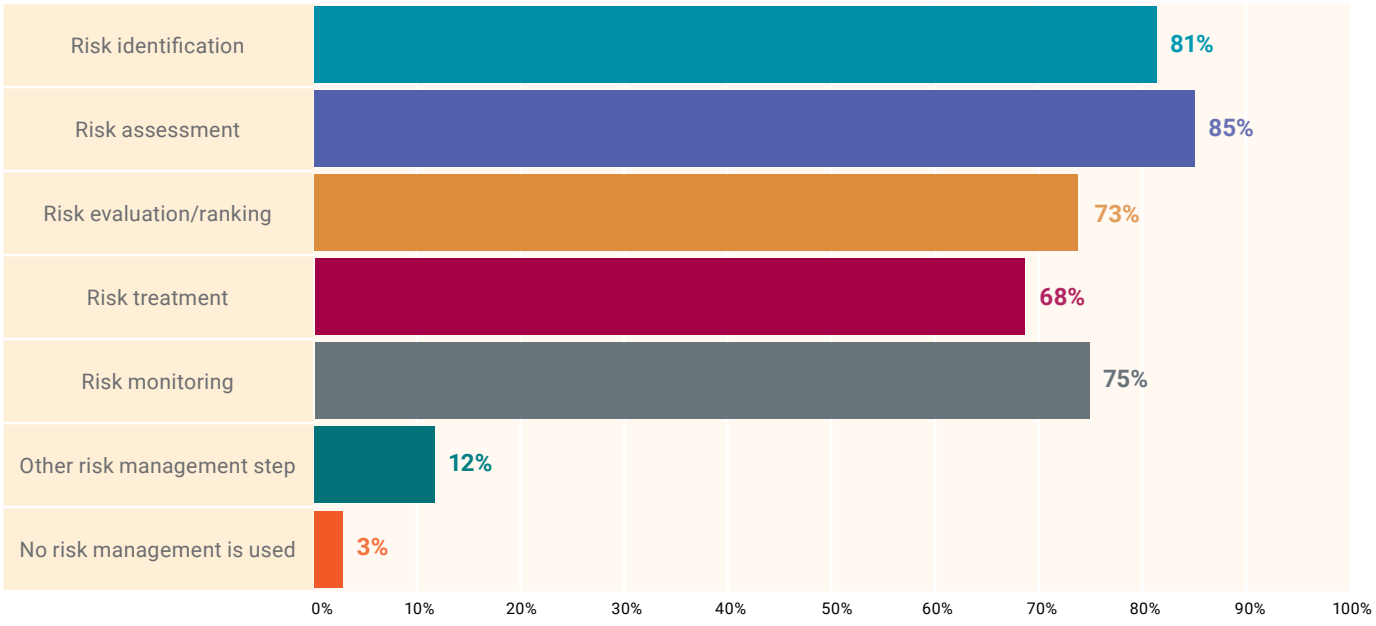
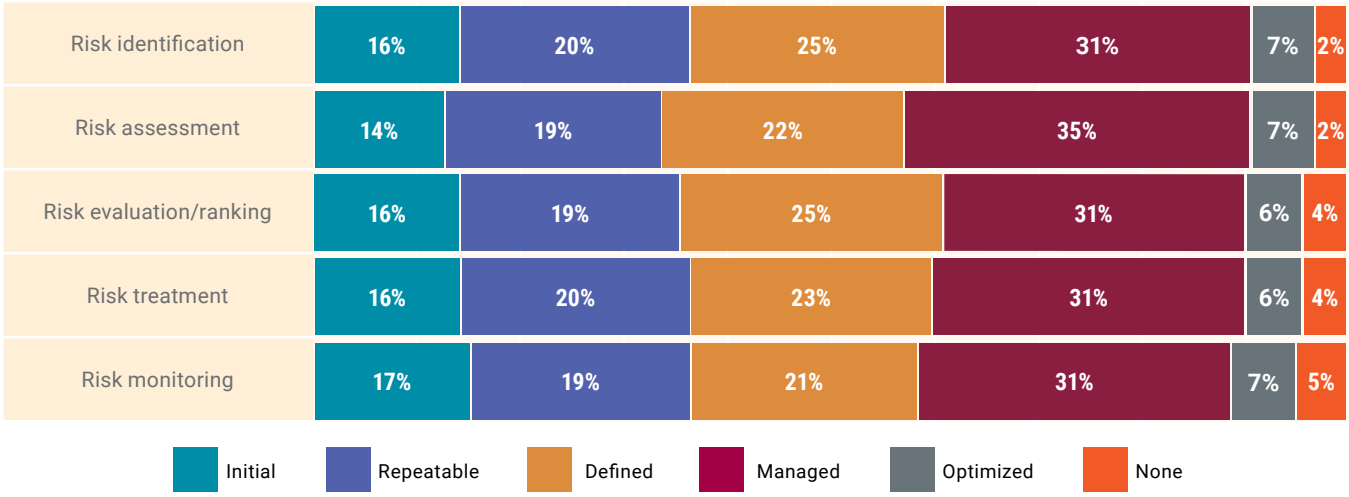


FIGURE 7—MATURITY OF RISK MANAGEMENT PROCESS STEPS
For each of the following risk management phases, please rate the maturity of your organization on a scale from None (least mature) to Optimized (most mature).



A thorough understanding of the risk tolerances—the minimum risk (floor) that should be undertaken in pursuit of business goals and the maximum acceptable risk (ceiling)—is key to risk management and operation of the business generally. A possible opportunity for enterprises that struggle with the maturity of their risk management may be to look to refining and clearly defining risk tolerances for their enterprise as they seek to advance along the maturity spectrum.

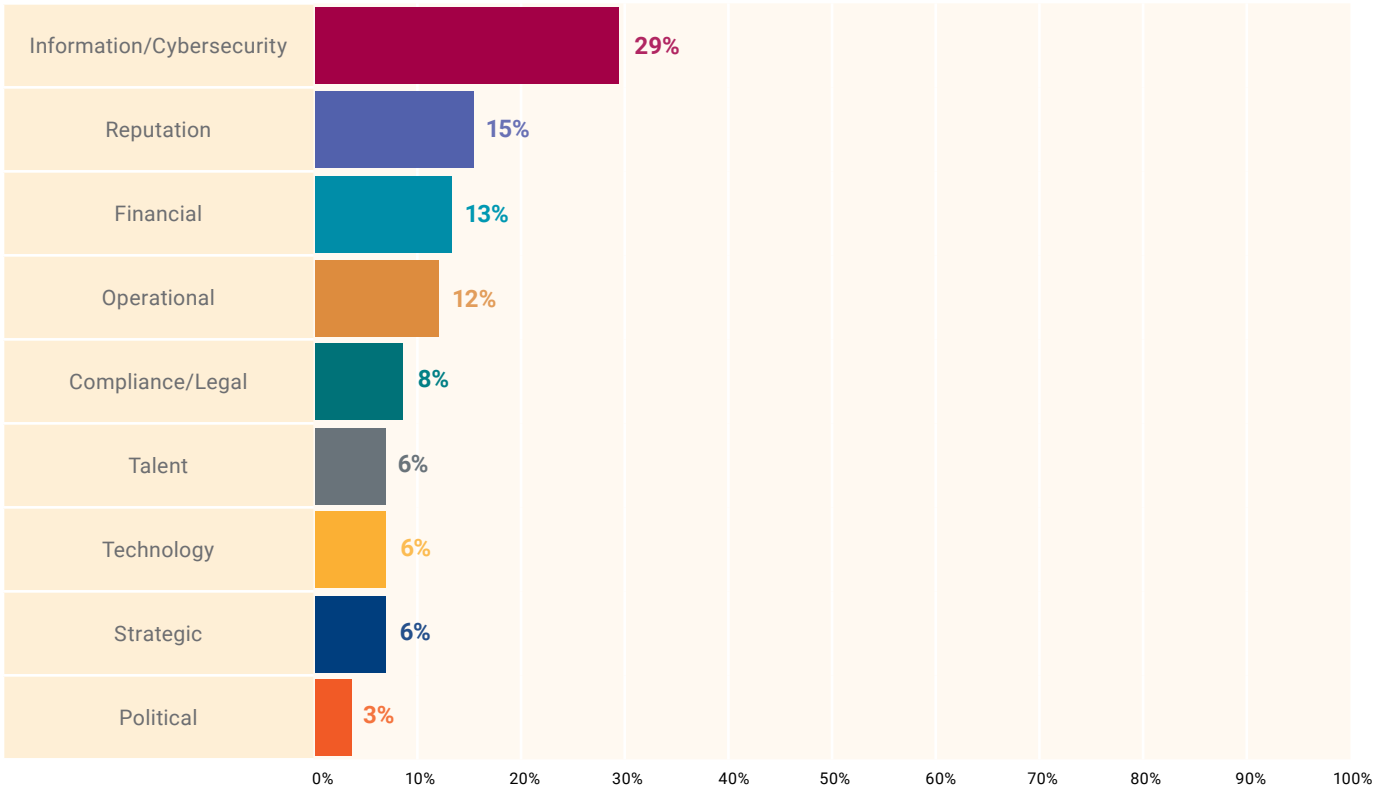
Adding to the challenge of improving the risk management process is the difficulty of forecasting certain types of risk, particularly when viewed through a geographic or industry lens, i.e., individual regions or industries may be more susceptible to certain types of risk. For example, statistically significant upswings in political risk are observed in the UK (this might be Brexit related) and India. Likewise, the type of business may impact risk; for example, operational risk is significantly more difficult to forecast for manufacturing and engineering market segments compared to other industry segments. Cybersecurity and technology risk, by contrast, are hardest (by a wide margin) to forecast for the financial services sector and insurance. Regionally, the United States and India have the most difficulty with forecasting compliance and regulatory risk.

Cybersecurity Risk Is an Emerging and Key Challenge Area

Most risk managers intuitively understand that cybersecurity is a significant area of risk for their enterprises. Survey respondents report information/cybersecurity risk as the most critical risk category facing their enterprises; it is cited as the single most critical risk, with almost double the percentage of the next closest critical risk type (29 percent, compared to a distant second-place reputational risk at 15 percent), as shown in **figure 8**. Moreover, reputational risk, the second highest type of risk cited, can be a consequence of a cybersecurity risk.[2]

FIGURE 8—CRITICAL RISK TODAY

What is the most critical category of risk facing your organization today?

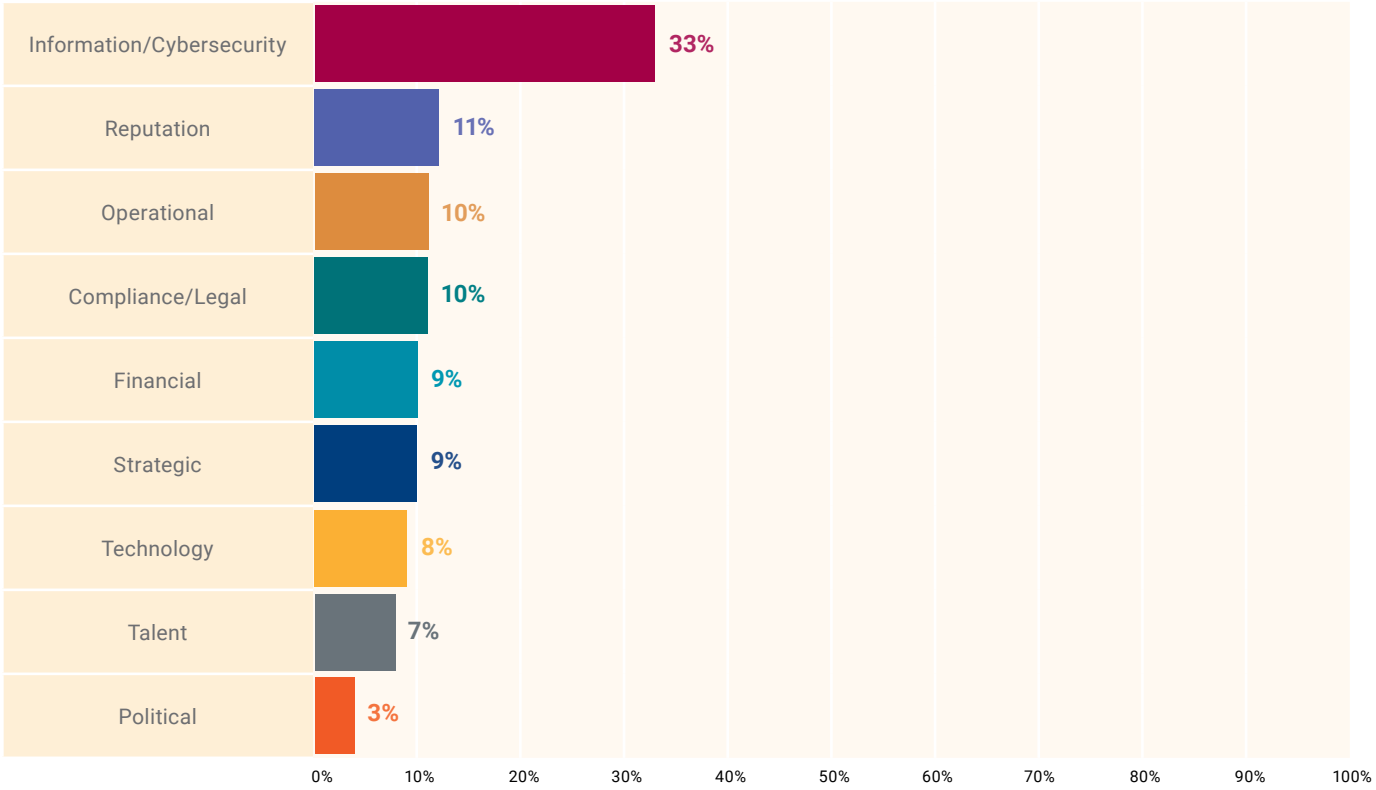


[2] A highly publicized breach may have reputational impact whose root cause is cybersecurity failure. It is worth noting that this is only sometimes true; an executive with legal troubles or an unpopular political opinion can be a reputational risk stemming from a non-cybersecurity related cause.

Survey respondents forecast that the most critical source of risk over the next 18 to 24 months is, again, information/cybersecurity, but the concern increases significantly. During this longer-term time horizon, 33 percent of respondents cite cybersecurity as the most critical risk category, while the nearest other critical risk category (reputational risk) is over 20 percent lower, at 11 percent (**figure 9**).

FIGURE 9—CRITICAL RISK IN 18 TO 24 MONTHS

What do you believe will be the most critical category of risk facing your organization in the next 18-24 months?



In addition to being the most acute risk pain point for enterprises, cybersecurity represents one of the most challenging risk types for respondent enterprises to define and assess objectively. Reasons for this challenge include everything from the mercurial surface of the threat landscape and the complexity and dynamic nature of the technology landscape within enterprises to issues related to finding and maintaining the right staff with the right skills. This may not be entirely unexpected, but more surprising is the ubiquity—across regions, countries and industries—associated with cybersecurity challenges and the organizational difficulties in meeting them.

Cybersecurity was also cited as one of the most difficult risk categories to define and assess (**figure 10**). Cybersecurity is also one of the most difficult risk categories to mitigate (**figure 11**). Survey respondents indicate that other risk types—strategic risk, reputation risk and political risk—are harder to measure than cybersecurity risk (**figure 12**), suggesting that although cybersecurity is a challenge, it is at least an understood challenge.

FIGURE 10—DIFFICULTY OF DEFINING AND ASSESSING RISK

For each of the following risk categories, how difficult, if at all, is defining and assessing risk?

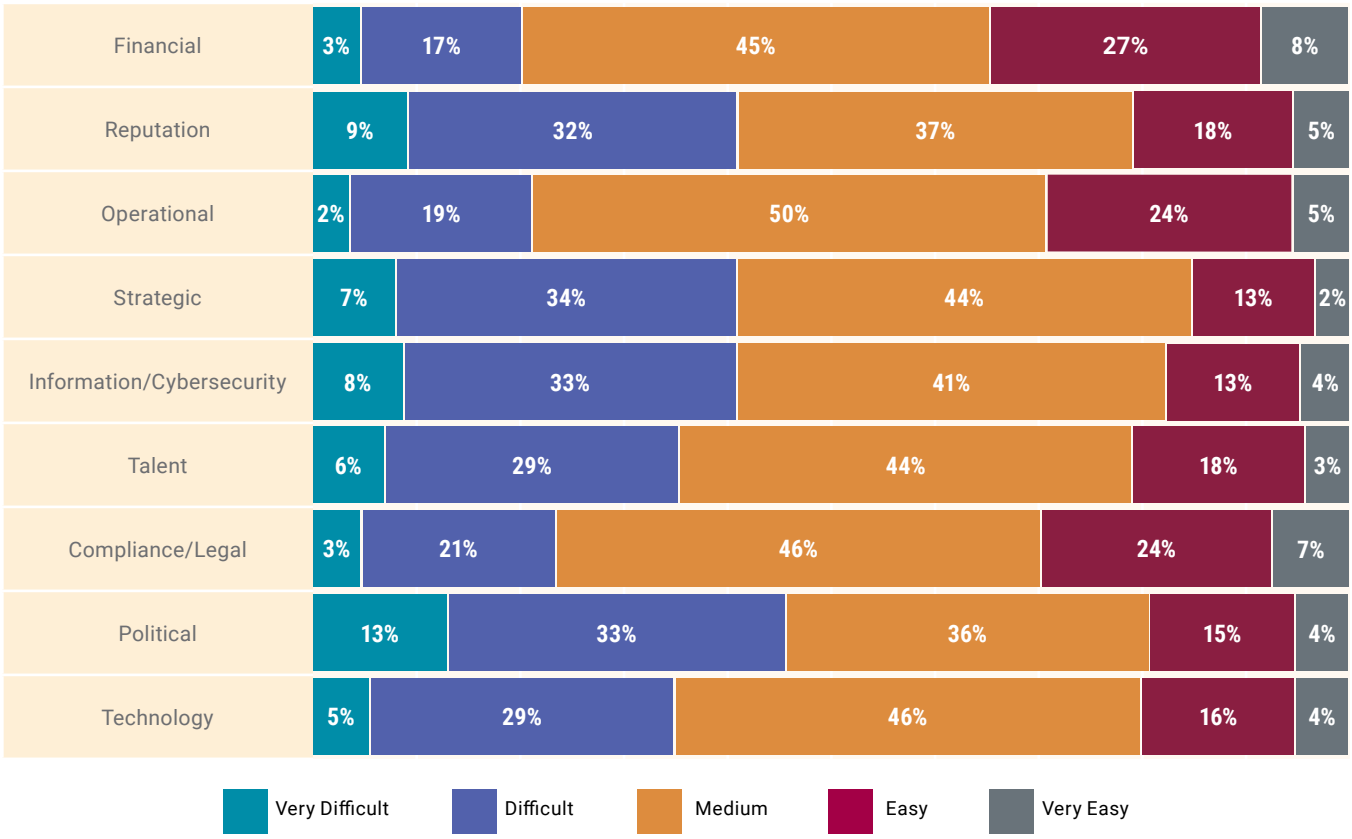


FIGURE 11–DIFFICULTY OF MITIGATING RISK

For each of the following risk categories, how difficult, if at all, is mitigating risk?

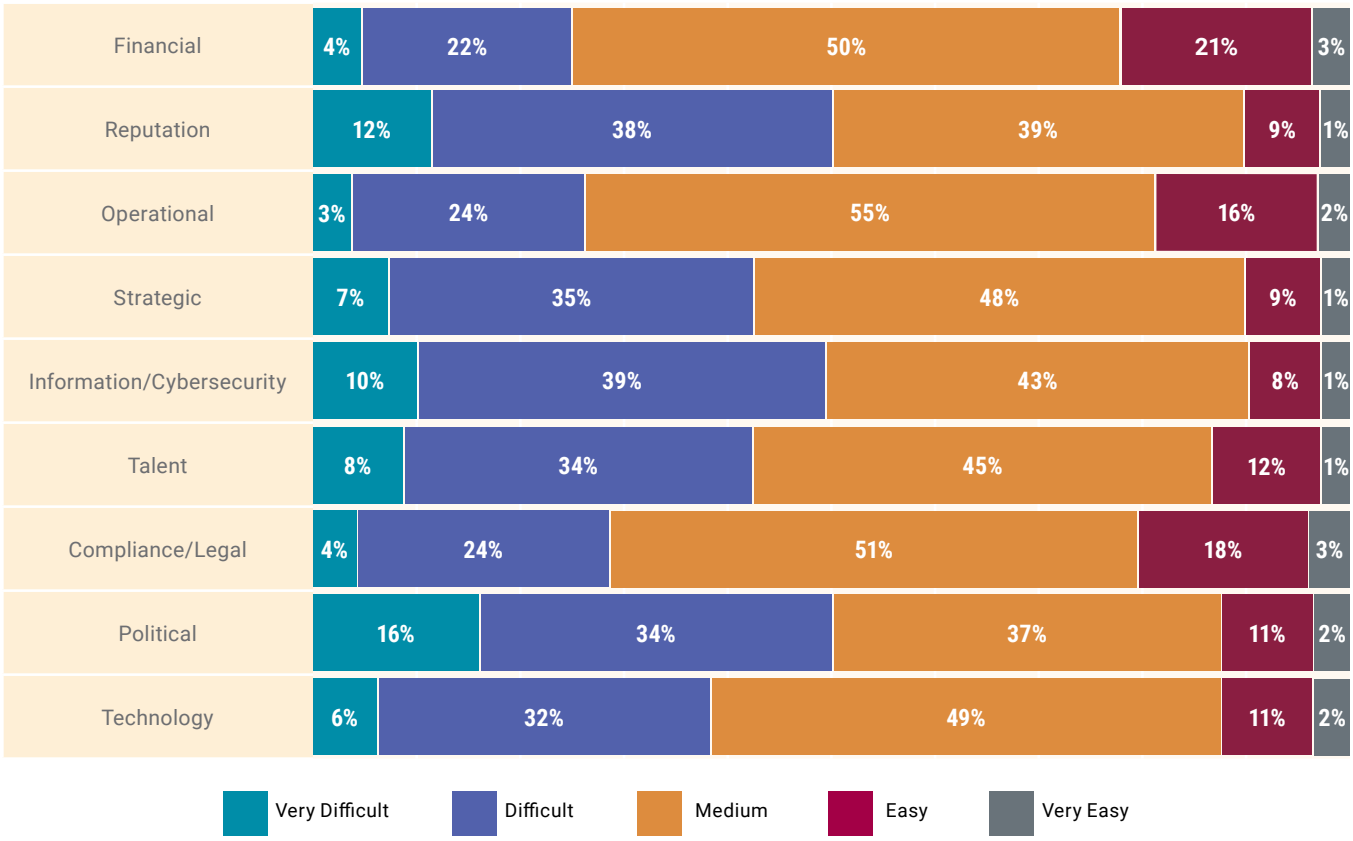
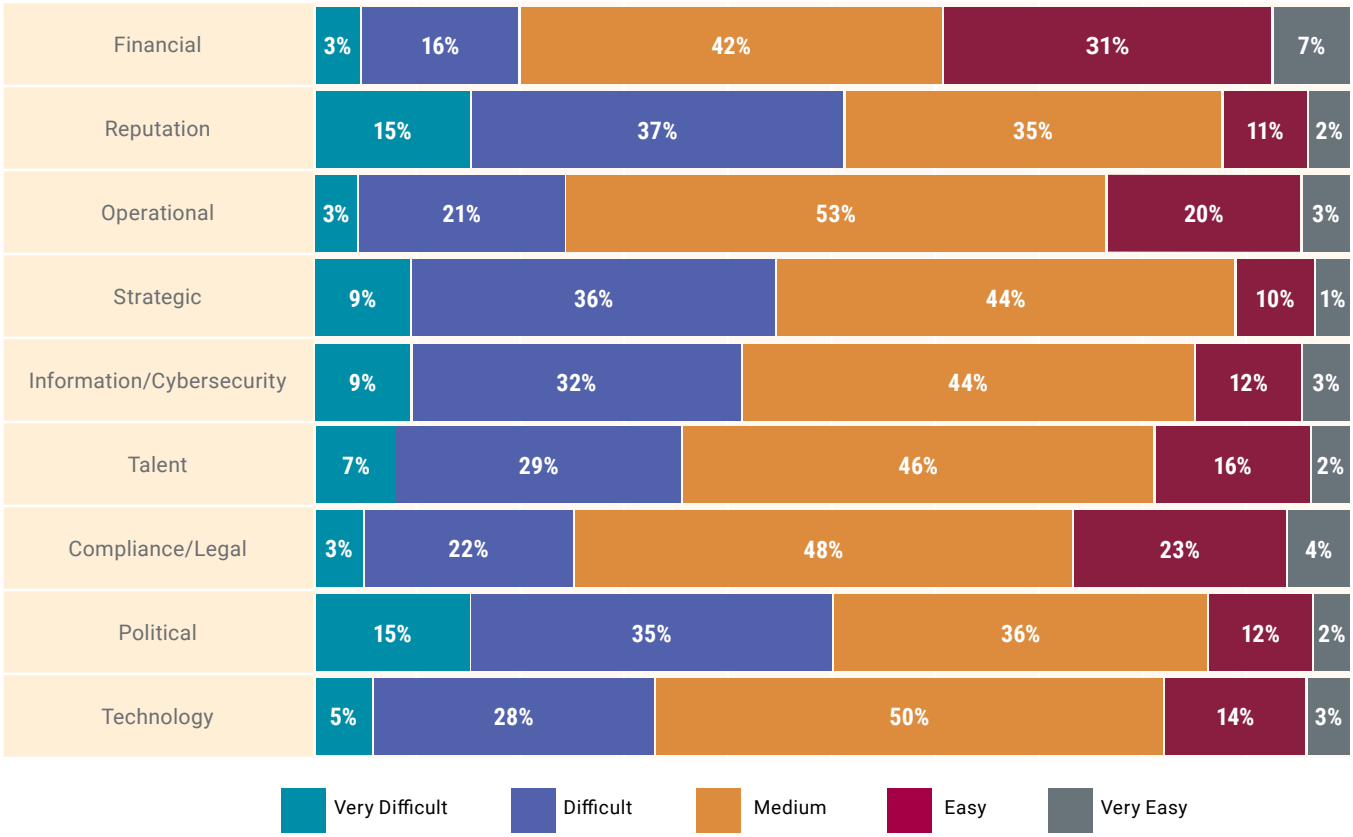


FIGURE 12—DIFFICULTY OF MEASURING RISK
For each of the following risk categories, how difficult, if at all, is measuring risk?

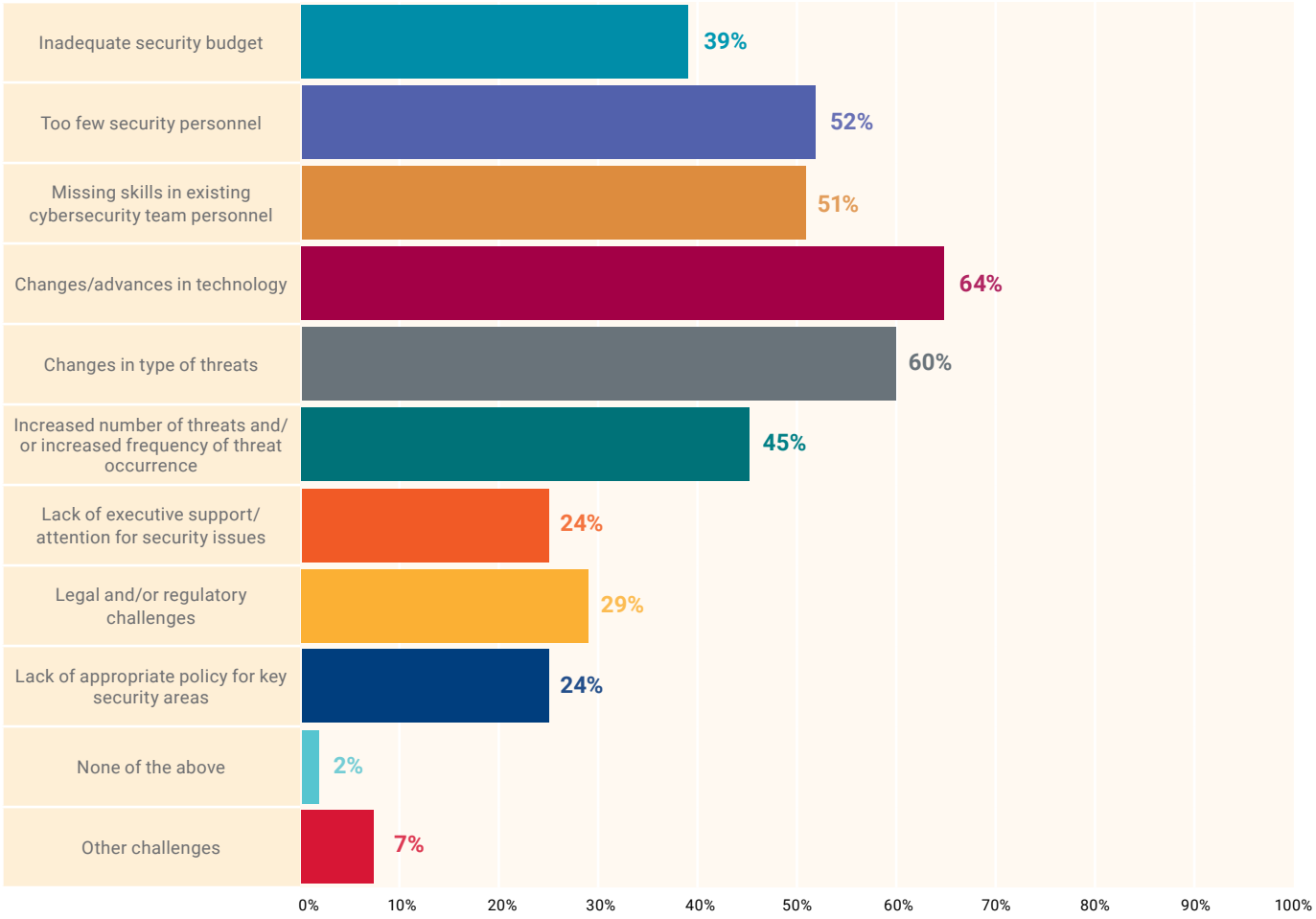


Part of the issue compounding these challenges may be a potential disconnect between management and governance of enterprises in the reporting of cybersecurity risk. The survey results show that boards of directors are generally updated about cybersecurity risk relatively infrequently—on a quarterly or less frequent basis (81 percent are updated quarterly, annually or without a set schedule)—while chief information security officers (CISOs) are updated much more frequently (70 percent are updated monthly or more frequently). At an operational level, reporting is also happening more frequently (68 percent are updated monthly or more frequently), but one area of opportunity may be to expand visibility to the governance level beyond its current level. Note that there is a geographic component to reporting. CISOs in Asia and Latin America are notified less often than the aggregate, while boards in Oceania, Europe and Asia are updated somewhat more frequently than the aggregate.

Survey respondents identified the cybersecurity challenges that their enterprises currently face. Implicit in this survey question is to identify the types of challenges related to cybersecurity that are the most problematic. The most concerning areas for the majority of enterprises are the pace of change of the technology landscape, i.e., new advances in technology (64 percent), and changes in the threat landscape, i.e., new types of attacks and vulnerabilities (60 percent). Too few security personnel (52 percent) and missing skills in existing cybersecurity team personnel (51 percent), representing the often-cited cybersecurity skills gap,[3] are the next top concerns (**figure 13**).

FIGURE 13—CYBERSECURITY CHALLENGES TODAY

Today, which, if any, cybersecurity challenges does your organization experience? Select all that apply.

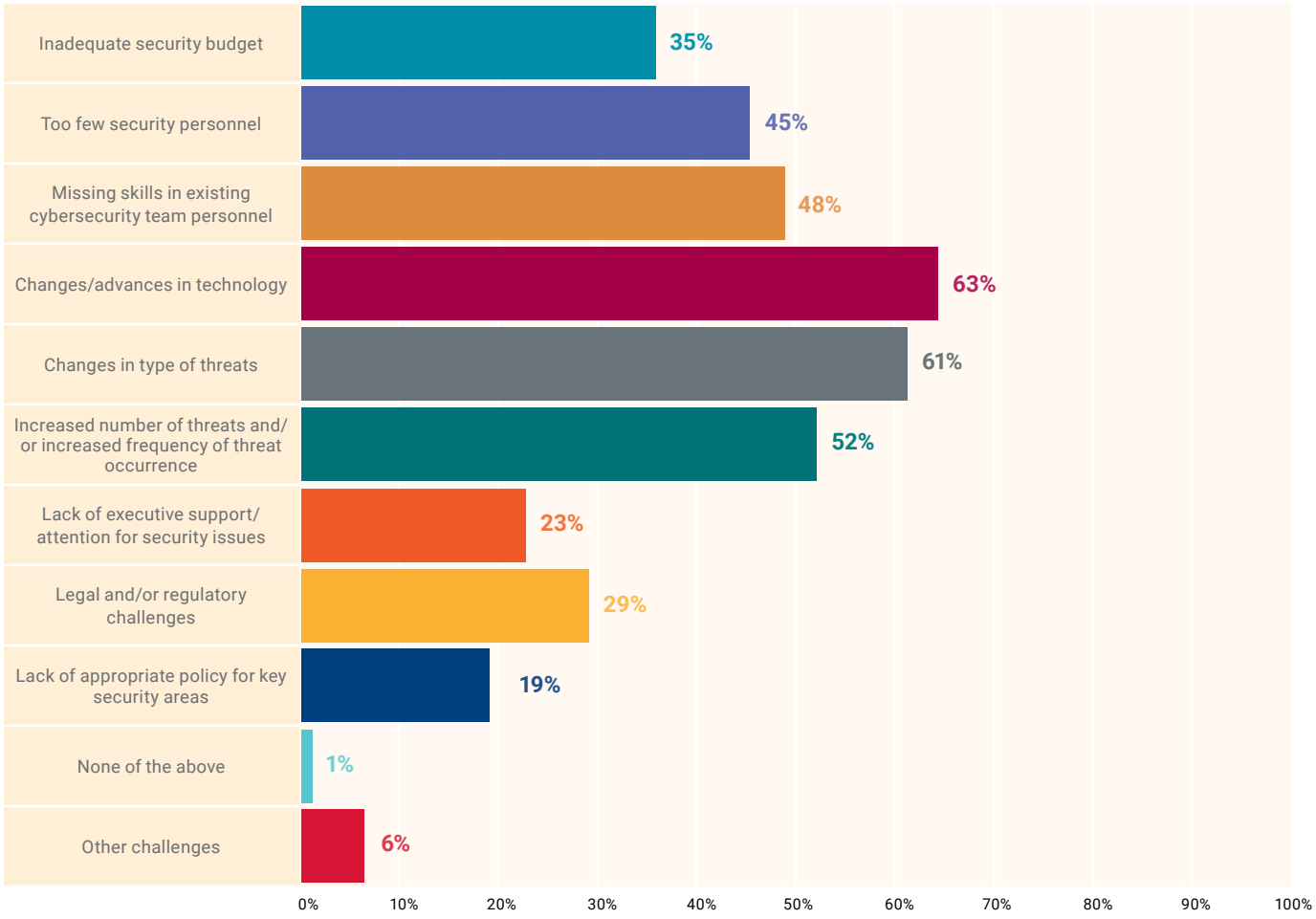


[3] ISACA®, *State of Cybersecurity 2019, Part 1: Current Trends in Workforce Development*, USA, 2019, https://www.isaca.org/info/state-of-cybersecurity-2019/index.html

Interestingly, when asked about these cybersecurity challenges over the next 12 months, survey respondents say that skill-related challenges are less concerning relative to other types of challenges (**figure 14**). Over the next 12 months, respondents expect changes/advances in technology (63 percent) and changes in type of threats (61 percent) to continue to be the top cybersecurity challenges. Increased number of threats and/or increased frequency of threat occurrence takes the third position at 52 percent.

FIGURE 14—CYBERSECURITY CHALLENGES EXPECTED IN NEXT 12 MONTHS

In the next 12 months, which, if any, cybersecurity challenges do you expect your organization to experience? Select all that apply.

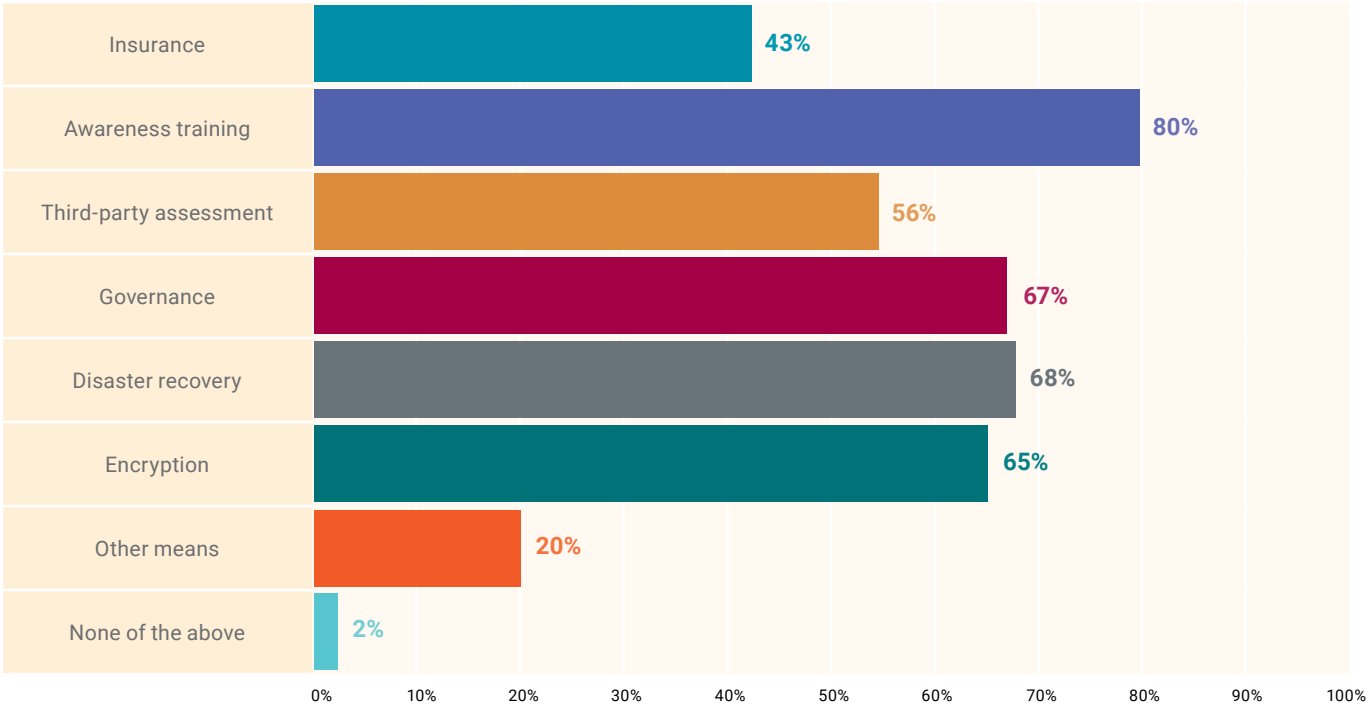


Half of the survey respondents (50 percent) believe that their enterprises have been impacted either significantly or moderately by nation-state sponsored attacks. Regionally, Asia, particularly India, has the highest percentage of respondents with that belief. Respondents in North America, Oceania and Europe are less likely to report potential impacts from nation-state sponsored cyberattacks. Among the respondent industries represented in the survey results, respondents in the financial, government and insurance industries are more likely to believe that their enterprises are negatively impacted by nation-state sponsored cyberattacks than respondents in other industries.

Regarding a potential cybersecurity failure in their enterprises, survey respondents are most concerned with a negative impact to the reputation, operational and technology risk categories, with reputation risk receiving the most concern. To mitigate potential cybersecurity failures, survey responses indicate that security awareness training is the most frequently deployed mitigation control (**figure 15**). Eighty percent of respondent enterprises have awareness training in place, followed by 68 percent that use disaster recovery strategies and 67 percent that employ generic governance controls. Less than half of respondent enterprises employ insurance as a mitigation control; North America and Africa are the highest adopters of insurance.

FIGURE 15—TOP MITIGATION CONTROLS

What are the top mitigation controls in place in your organization today to protect against a critical cybersecurity failure? Select all that apply.



Cloud-related Risk Concerns Forecast Similar Concerns for New and Emerging Technologies

Cloud, as one would expect, is a significant pain point for many enterprises and a key source of potential new risk. Although cloud is no longer an emerging technology because most enterprises have adopted it extensively, the trajectory of cloud—both adoption dynamics and risk introduced—can serve as a bellwether for other, newer technologies. By looking at more nascent technologies in earlier stages of adoption, e.g., AI and IoT, risk is beginning to emerge that is specific to those technologies in industries where usage is more prolific relative to others. Given the pain point that cloud (a more mature technology) represents for enterprises today, it is likely that these newer emerging technologies will become a more pronounced source of risk for enterprises, as the usage of these technologies proliferates and as adoption becomes mainstream.

A particularly interesting survey finding is the impact that emerging technologies have had on the overall risk posture of enterprises. At first glance, the data seem straightforward. When asked about the impact of new technologies on the enterprise risk profile, respondents most often cite cloud as increasing threats and vulnerabilities (70 percent). There is a good reason why the cloud percentage is so high—practitioners are intimately familiar with the challenges of cloud, including compliance and regulatory challenges, data sovereignty, lack of direct operational control over service provider environments, shadow adoption, and numerous other pain points. However, and perhaps unexpectedly, respondents cite other technologies—Internet of Things (IoT) (34 percent), machine learning and artificial intelligence (AI) (25 percent), and blockchain (13 percent)—significantly less as sources of potential new vulnerabilities and threats (**figure 16**). Indeed, respondents indicate that some new technologies, like AI, have use cases that help to decrease vulnerabilities and threats, i.e., helping to bolster cybersecurity efforts or reduce overall risk through their use (**figure 17**).

Technologies other than cloud, such as artificial intelligence, blockchain and IoT, are in a state of relative infancy compared to the strong adoption of cloud. The survey data become significantly more interesting and nuanced when technology usage is accounted for, particularly when approached through an industry lens. In the industries where a higher adoption of a particular technology is expected, the threats and vulnerabilities from that technology are perceived as greater. For example, IoT applications are cited by respondents as a significantly greater cause of threat/vulnerability expansion in manufacturing and technology services, where the adoption of these technologies is expected to be higher. Likewise, machine learning and AI impacts are reported as highest in financial services and insurance, where adoption rates are expected to be higher; and blockchain impacts are highest in financial services, insurance and technology services, as expected. Therefore, technology impact on risk correlates (at least loosely) to increases in usage and adoption.

This impact is concerning. If it is the case that an increase in adoption correlates to a perceived increase in vulnerabilities and threats facilitated by the technology, this, in turn, points to a possible future upswing in sources of new vulnerabilities and threats as these newer technologies become more adopted. If a similar trajectory of new security concerns and potential risk areas associated with these technologies can be expected as they mature, this points to numerous areas of potential concern for risk practitioners on the horizon.

FIGURE 16—EMERGING TECHNOLOGIES THAT **INCREASE** RISK

Of the following emerging technologies, which, if any, have increased the level of threats and vulnerabilities within your organization as a result of their use? Select all that apply.

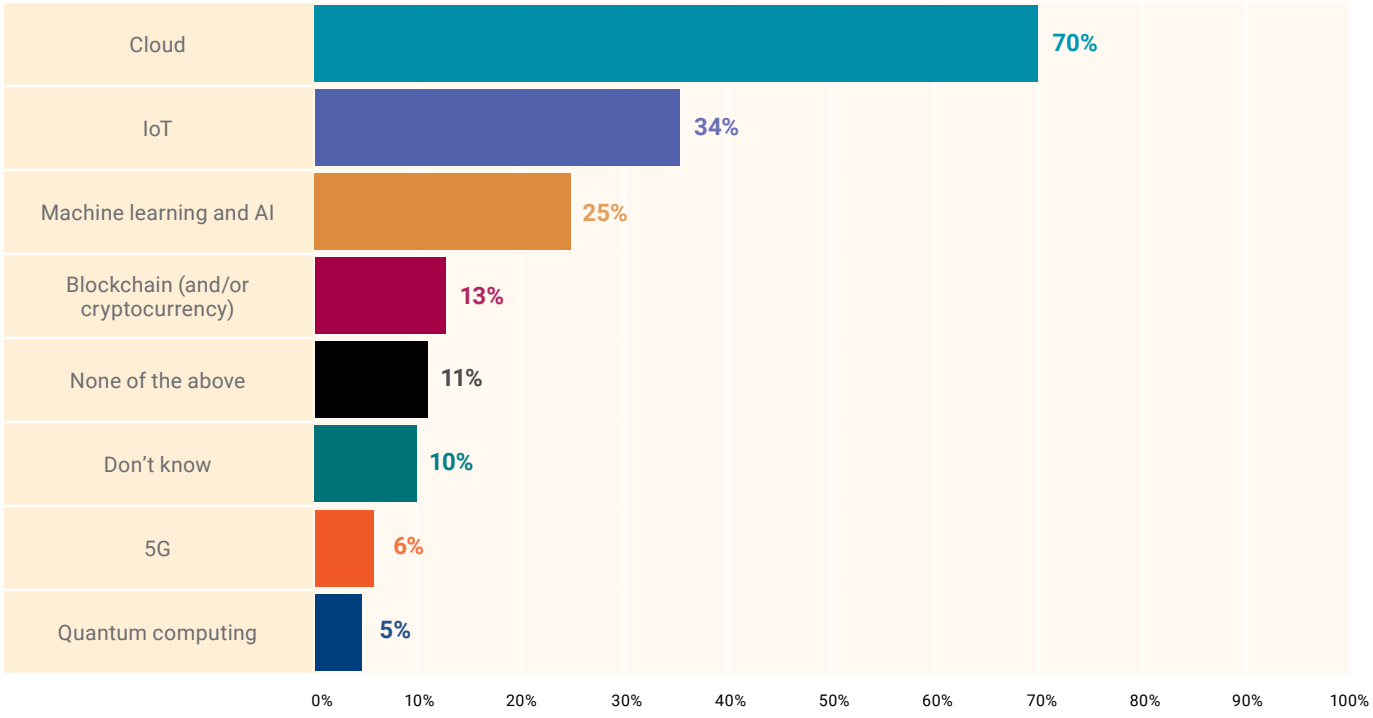
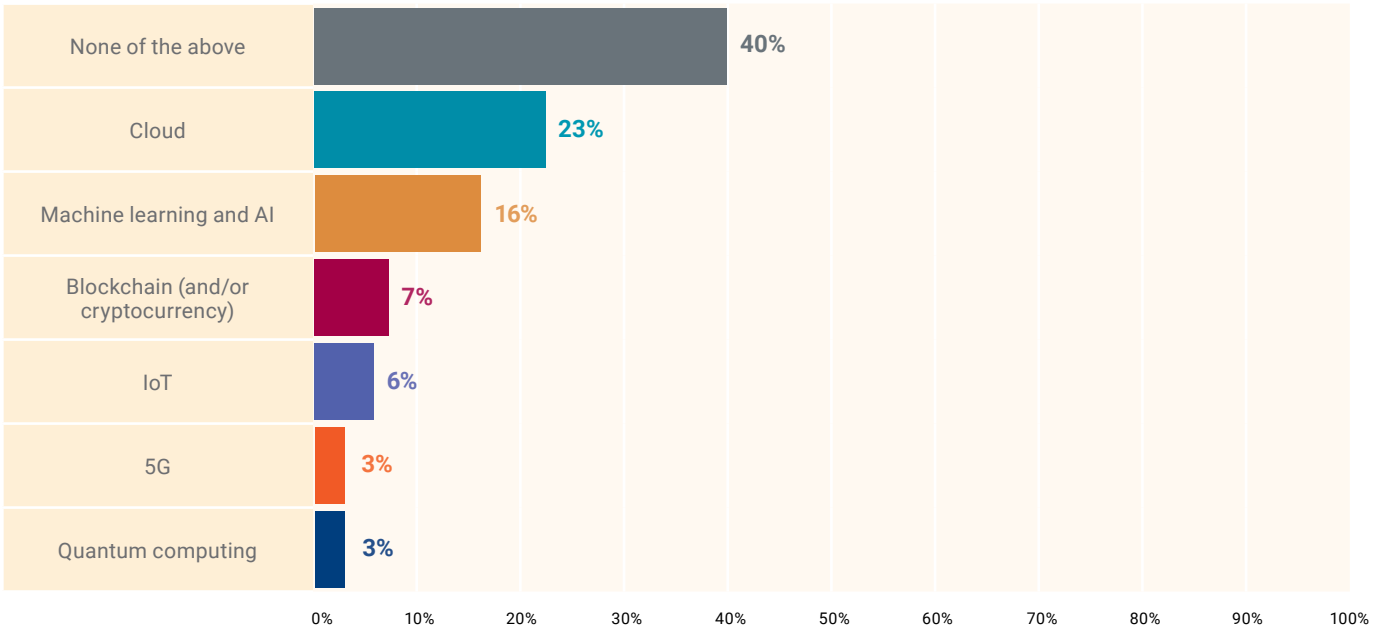


FIGURE 17—EMERGING TECHNOLOGIES THAT **DECREASE** RISK

Of the following emerging technologies, which, if any, have reduced the level of threats and vulnerabilities within your organization as a result of their use? Select all that apply.



This may be, in part, due to challenges that survey respondents see in the ability of their enterprise to accurately predict the potential impacts associated with new technology use. Only 31 percent of respondents are extremely or very confident in the ability of their enterprise to accurately predict new-technology impact. There is a regional component to this; for example, respondents in India and the United States are most confident in the ability of their enterprise to predict these impacts. Also, respondents in some industries (government, technology services and financial services) are more confident relative to their peers in other industries.

If enterprises are not able to accurately predict threats and vulnerabilities associated with emerging technologies, they may need to become nimbler regarding the speed of mitigation associated with these potential issues. Although more than half (60 percent) of respondent enterprises can put mitigations in place within three months of the identification of a new vulnerability or threat, these numbers are not optimal. In fact, only 31 percent of respondents indicate their enterprises can respond most quickly (less than one month) to the identification of a new area of concern (**figure 18**).

The survey results for the time to mitigate risk are similar to the results regarding the relative responsiveness of executive teams to new mitigation tactics after the identification of these new issues. Only slightly more than half (57 percent) of survey respondents report that their executive teams are either very or extremely responsive to new mitigation tactics after the identification of new threats or risk (**figure 19**).

FIGURE 18—MITIGATION TIMELINE FOR NEW TECHNOLOGY THREAT OR VULNERABILITY

Once a new technology threat or vulnerability is identified, how long (on average) does it take your organization to put countermeasures in place to mitigate it?

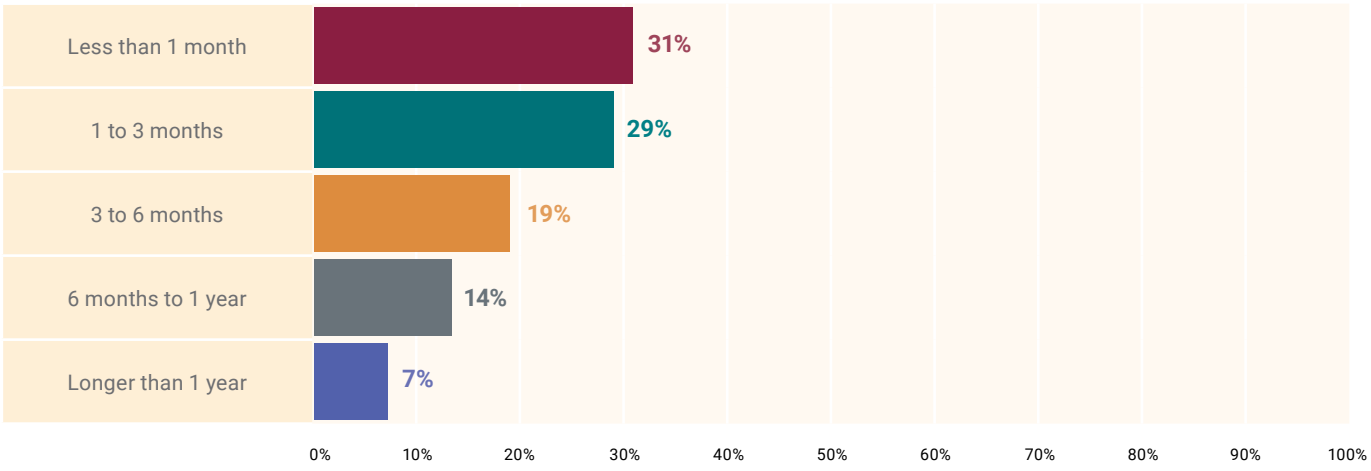
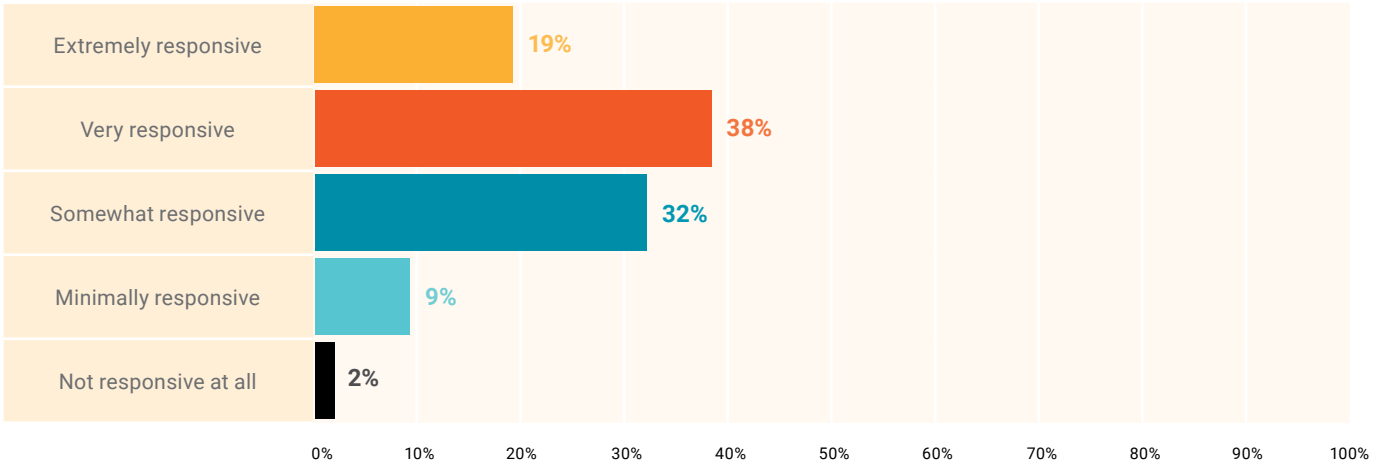


FIGURE 19—EXECUTIVE RESPONSIVENESS TO NEW MITIGATION TACTICS
How responsive is your executive team or board in supporting new mitigation tactics after a critical technology threat or vulnerability is identified?



Although Technology Risk Is High, Traditional Risk Remains a Concern

Cybersecurity and technology risk observed in the survey results are noteworthy, but it is also useful to point out that other types of risk are also important to respondents and, therefore, deserve balanced scrutiny regarding risk management measures. It is particularly interesting to look at types of risk that are most concerning to respondents today and in the next 18 to 24 months through an industry lens.

Although financial services respondents are particularly alert to cybersecurity risk (citing it as a concern today at a percentage that is higher than other industries), other types of risk have particular importance for other industries:

- Respondents in the manufacturing industry cite operational risk as critical at a percentage that is higher than other industries (18 percent today, 16 percent in 18–24 months).
- Respondents in insurance firms cite compliance and regulatory risk more frequently than other industries (12 percent today, 13 percent in 18–24 months).
- Respondents in the manufacturing industry cite strategic risk more often than respondents in other industries (12 percent today, 13 percent in 18–24 months).
- Respondents in government cite political risk at a higher percentage than other industries (8 percent today, 7 percent in 18–24 months).

Looking forward 12 months, these patterns and percentages persist in respondent answers when asked to extrapolate future critical risk areas.

The industry-specific results are not surprising given the activities of those industries and the contexts in which they operate. Beyond industry, geography also plays a role in the specific risk that is deemed by respondents to be most critical.

Respondents in some regions report particular types of risk as being more concerning. Notable observations include:

- Increased criticality of reputational risk in Oceania and Europe
- Financial and operational risk in Africa and Latin America
- Compliance risk in Asia and Europe
- Technology risk in Africa and Asia
- Political risk in Africa

Locale-specific factors (e.g., regulatory climate) play a role in determining the most critical risk type. Like the industry-focused view, patterns continue when respondents are asked to cite the risk most critical in the future. One noteworthy exception to this is an expansion in criticality associated with strategic risk in Latin America—appearing at a significantly higher rate than other regions for future risk but not showing statistically significant differences for risk today.

Road Map for a Risk-optimized Enterprise

The goal of effective risk management is not always to completely remove risk. Risk, when judiciously and strategically undertaken, can lead to competitive advantage, opportunities to better achieve the enterprise mission, entering new markets and numerous other advantages. Instead, the goal should be to ensure that the right risk is being taken in a manner that is judicious and alert to the possibility of potential failure, while ensuring that unnecessary risk—or risk that is out of conformance with the enterprise risk appetite—is avoided.

Based on the insights from this survey, there are several ways that enterprises can hone and improve their risk management efforts to best achieve this result. These are:

- Enhance performance of risk management, including advancing the maturity of risk management processes where appropriate
- Infuse risk understanding into the grass roots
- Address current pain points and create a bulwark against likely future problem areas
- Take concrete actions at the management level to better integrate risk management into the enterprise

Enhance Performance of Risk Management

As previously noted, risk management practices have room to improve in the steps that are taken and the maturity of the processes in use. The most fundamental risk management steps are close to ubiquitous—or at least very well adopted (i.e., 85 percent of enterprises employing risk assessment and 81 percent employing risk identification). However, other steps in the process are less employed (e.g., risk treatment and risk evaluation).

There is some room for improvement in terms of what steps are taken in the risk management life cycle, but the most room for improvement is in the maturity of the processes used. This is because maturity of risk management steps is not where one would expect them to be in light of the perceived criticality of risk and the potential impacts. This observation in no way suggests that it would be appropriate for every enterprise to work toward the highest maturity level for every risk management step. To the contrary, many enterprises may reasonably conclude that a fully optimized process for every step in the risk management life cycle is too time intensive or too costly an undertaking for them to reasonably implement and, therefore, decide a lower level of maturity is

right for them. There are still some benefits associated with moving away from ad-hoc processes toward a workmanlike, systematic, documented and repeatable methodology for risk management.

Primarily, ensuring that risk management steps are at least documented directly benefits the risk management process itself. More mature (and therefore more directly repeatable) processes allow enterprises to more consistently assess and treat risk. For example, the results of a risk assessment this year can be directly compared with prior years, as the methodology and processes used to derive the assessment remain constant over time. This means that enterprises can track improvements (or degradation) of the risk management process itself over time and track their overall risk profile over different points in time.

Additionally, more mature processes for risk treatment can help ensure that mitigation or treatment controls of comparable intent and rigor are selected between executions of risk management/treatment steps. This, in turn, means that controls selected are of comparable quality regardless of who undertook the step, who selected the control, etc.

For enterprises wishing to optimize their risk posture, therefore, moving to more mature processes can be used to directly bolster their understanding of risk and thereby lead to better optimization of risk for their enterprises.

Infuse Risk Understanding Into the Grass Roots

As noted previously, awareness of risk facing the enterprise directly correlates to the position of respondents in the organizational hierarchy. More senior personnel are more directly aware of the risk environment faced by the enterprise of which they are a part. This is not necessarily desirable, given that execution of business strategy, elements of operational responsibility, interaction with customers and other key aspects of running the business are almost certainly likely to occur at all levels of the organizational reporting chain. No matter how well and carefully thought out a risk management strategy is then, opportunities arise for that strategy to be subverted when key participants in execution (i.e., those lower in the hierarchy) are unaware of the nature and scope of the problems being solved and what measures are in place to ensure that negative outcomes do not come to pass.

It can be beneficial to expand risk awareness to all levels of the organizational hierarchy and enlist the assistance of more junior resources in executing the risk optimization strategy. For example, a campaign of grass roots risk awareness targeting those less-senior individuals about the nature of the risk that may face the enterprise (and strategies the enterprise has in place to combat them) can help ensure that appropriate steps are followed, that diligence is applied to execution of risk treatment steps, and that any areas of oversight (e.g., where controls are not operating the way that they should be operating) are noted and reported upward.

Care should be exercised in the specificity of information being shared (for example, one may not wish to share detailed mergers and acquisitions or financial information with everyone in the firm), but an appropriately transparent discussion (even if high level where details are redacted) can be beneficial in enlisting the assistance of others to support risk management efforts.

Address Current Pain Points and Create a Bulwark Against Likely Future Problem Areas

Several pain points, such as cloud and cybersecurity risk, are noted throughout this research brief. However, bearing in mind that the full risk associated with cloud may be a foretaste of future risk associated with newer and less mainstream technologies, such as AI, IoT and blockchain, it may be beneficial for enterprises to leverage this fact to start addressing these technologies from a governance and risk management point of view before impacts become overly widespread.

There is no one-size-fits-all model for how to do this. A manufacturing company that has already started the process of adopting IoT technologies may be further along the adoption curve than an enterprise that is in another business, such as retail or insurance. A combination of technology

discovery (i.e., looking for and tracking efforts to leverage these newer technologies in the enterprise) coupled with candid conversations and open-minded thought about the impact of these technologies can potentially help spare pain down the road as these technologies become more mainstream.

After discovery occurs, a systematic approach to forecast potential risk areas that may arise through the use of technology can help enterprises—particularly those that may be slow to respond to new threats when they are identified—take action in a timely enough fashion to keep the enterprise protected.

Take Concrete Actions at the Management Level to Better Integrate Risk Management Into the Enterprise

Finally, oversight and execution of risk management can be better integrated into the overall operation of the business. This is true from both a governance and management point of view. Certain risk areas, such as cybersecurity risk, are not communicated to boards in a manner timely enough for them to respond—for example, when they are informed about cybersecurity risk only infrequently.

However, it is at the management level where the broadest opportunity for improvement can be realized. The timeline for acting on newly identified risk is not what it could be, in some cases allowing months to pass before countermeasures are implemented. Likewise, support for mitigation tactics at the executive/board level has room to improve, as 89 percent are (at best) somewhat responsive to taking direct action. Finally, vague or undefined risk expectations from the top, i.e., at the governance (board) level or from senior management, can lead to inappropriate mitigations (either overly constricting or overly permissive.) This is particularly true given that risk is generally less well understood the lower down in the organizational hierarchy one goes. Therefore, clear and direct expectations about risk tolerance—along with corresponding guidance for those personnel who may be expected to make risk decisions for the firm—can go a long way to helping optimize risk for the enterprise over the long term.

Conclusion

It is perhaps not a surprise to risk practitioners, i.e., those practitioners with a stake in analyzing, mitigating, assessing, triaging or otherwise making decisions about risk for their enterprises, that risk on the whole is increasing. It is further probably not surprising, given a cursory look through the trade media headlines, that threats are becoming more prevalent and that changes in technology and threat landscape have an impact on this risk.

There is significant value associated with a careful examination of both the risk and the risk management processes and steps used by enterprises to address them. Looking at how and why this risk is increasing—as well as examining how enterprises react—is informative because it helps enterprises understand how they perform relative to peers, how they can improve risk management efforts, and how others in similar vertical industries or geographic regions handle risk management challenges that are still emerging.

As with anything, there is no golden ticket guidance that will work in every enterprise when it comes to risk optimization. However, the results from this survey can help enterprises make better decisions about risk, improve the measures they have in place currently and ultimately serve as data points to help guide their risk management development in the future.

Acknowledgments

ISACA would like to recognize:

ISACA Board of Directors

Brennan P. Baybeck, Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Rolf von Roessing, Vice Chair
CISA, CISM, CGEIT, CISSP, FBCI
FORFA Consulting AG, Switzerland

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Health Care Service Corporation, USA

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
introSight Ltd., Israel

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Rob Clyde
ISACA Board Chair, 2018-2019
CISM
Clyde Consulting LLC, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

Greg Grocholski
ISACA Board Chair, 2012-2013
CISA
Saudi Basic Industries Corporation, USA

David Samuelson
Chief Executive Officer
ISACA, USA

About ISACA

Now in its 50th anniversary year, ISACA® (www.isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

About CMMI Institute

A subsidiary of ISACA Enterprises, CMMI® Institute (cmmiinstitute.com) is the global leader in the advancement of best practices in people, process and technology. The Institute provides the tools and support for organizations to benchmark their capabilities and build maturity by comparing their operations to best practices and identifying performance gaps. For over 25 years, thousands of high-performing organizations in a variety of industries, including aerospace, finance, healthcare, software, defense, transportation and telecommunications, have improved their performance, and earned a CMMI maturity-level rating and proved they are capable business partners and suppliers.

About Infosecurity® Group

With over 23 years of experience in providing year-round education and networking opportunities for visitors, solution-providers and thought-leaders alike, the Infosecurity Group looks to bring the global infosecurity community together in person, in print and online. Featuring the award-winning Infosecurity Magazine as well as established events all around the globe, our purpose is to help you find "everyone and everything you need to know about information security."

Disclaimer

ISACA has designed and created *State of Enterprise Risk Management 2020* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505
Fax: +1.847.253.1755
Support: support.isaca.org
Web: www.isaca.org

Provide Feedback:
www.isaca.org/enterprise-risk-mgt-2020

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/