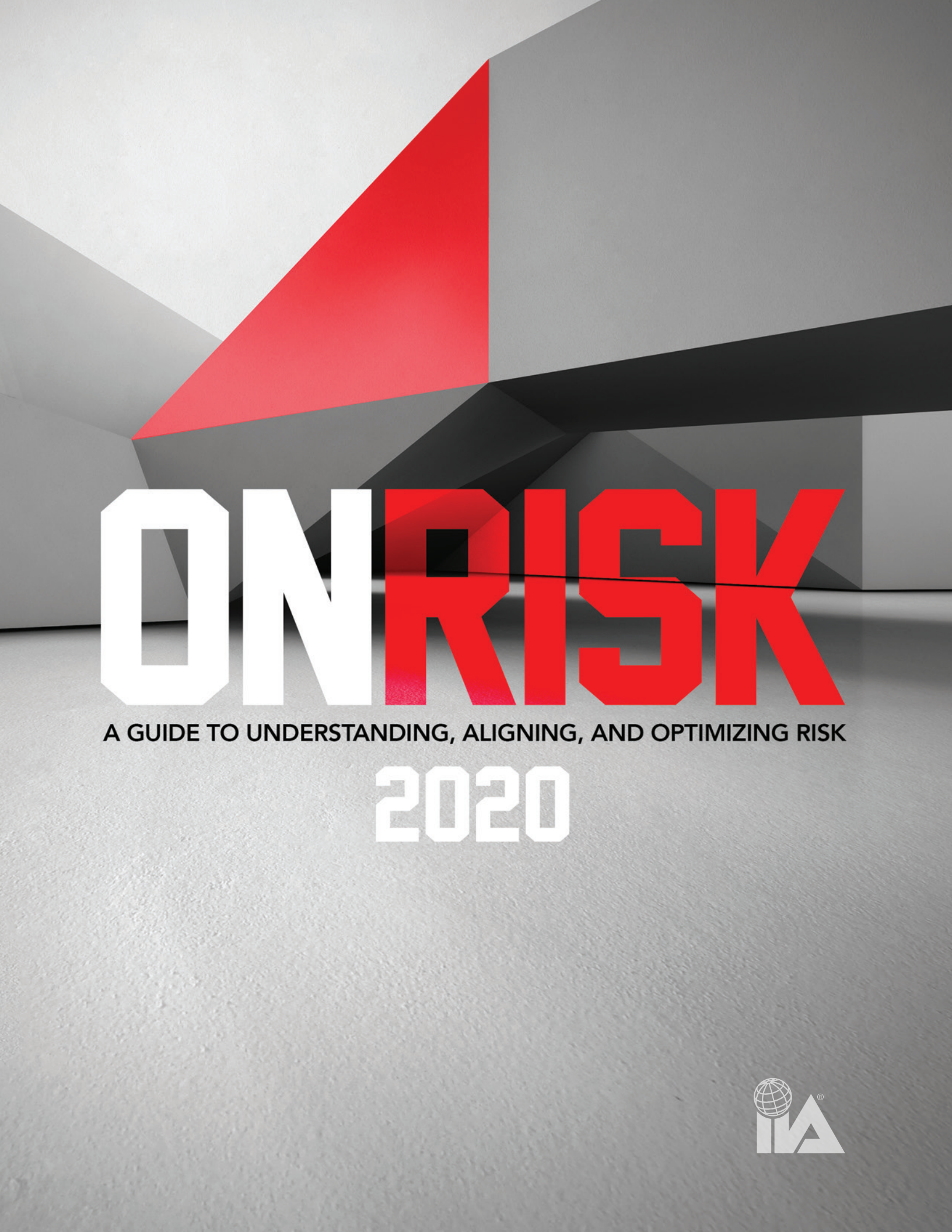


ON RISK

A GUIDE TO UNDERSTANDING, ALIGNING, AND OPTIMIZING RISK

2020

TABLE OF CONTENTS

Dear Readers,

I have the great pleasure of introducing the inaugural edition of an exciting new report from The Institute of Internal Auditors. ***OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk*** *is an innovative and insightful research report that promises to change the way organizations view and understand risk. That's a bold statement that requires some justification, so here it is.*

A number of risk reports published annually provide perspectives from individual players in the risk management process. However, no single report has provided a holistic view of risk from all perspectives — until now.

OnRisk 2020 *brings together the perspectives of the board, executive management, and chief audit executives (CAEs) on the risks that are top of mind for 2020 and beyond. Based on quantitative and qualitative surveys, the report lays out how each respondent group views key risks. Respondents shared their perspectives on their personal knowledge of the risks and their views of their organizations' capability to address the risks. But the most innovative and powerful benefit* ***OnRisk 2020*** *offers is a studied analysis of how those views differ and what that means to an organization's risk management.*

For example, the qualitative survey found that board members are consistently more optimistic about their organizations' capability to address key risks than members of executive management are. For some risks, board member views on capability were dramatically higher than those of executive management or CAEs. Taken together, these findings raise questions about how boards build their views on capability, and how this affects decisions that drive risk strategy.

Another example relates to managing cyber risk. Addressing this ubiquitous risk remains a daunting task, and its management is a top priority. Yet because of the ever-evolving nature of cybersecurity threats, executive management, boards, and CAEs are aligned in feeling that their knowledge of cybersecurity is low.

These insights should do more than just raise awareness of the misalignments, or gaps, that may exist. Through careful analysis of the survey data as well as additional research on each risk, The IIA has identified actions each respondent group may take to improve alignment with one another and ultimately enhance the organization's ability to address the risks. This is where ***OnRisk 2020*** *offers the most innovative and powerful benefit to organizations.*

Organizations should review the analysis and recommendations related to each of the 11 key risks that follow and are encouraged to conduct a similar review of the knowledge and capability perspectives among their own organization's board, executive management, and internal audit activity.

OnRisk 2020 *offers a robust look at key risks that organizations will face in the coming year, provides important benchmarking on capability to support risk and audit planning, and offers direction to help align and enhance risk management strategy and execution. I am confident you will find* ***OnRisk 2020*** *insightful, illuminating, and of immense value.*

Sincerely,

Richard F. Chambers

Richard F. Chambers
President and CEO
The Institute of Internal Auditors

INTRODUCTION

*Risk is a **thorny** word.*

In its simplest form, it means exposure to danger, but in an organizational or business context, it takes on a much more complex definition.

For generations, investors, boards, and executive management viewed risk as something to be avoided or mitigated, but organizations that take such a defensive posture cannot thrive for long in today's dynamic marketplace driven by global competition, rapid technological change, and geopolitical uncertainty. The modern approach to risk management must view risk as opportunity, as well. This requires strategic, coordinated, and seamless collaboration among key risk management players, and success in this arena demands a clear-eyed view of each player's understanding of and ability to leverage or manage risk.

The Institute of Internal Auditors (IIA) is proud to offer *OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk*, a robust and comprehensive view of the top risks for the coming year based on the perspectives of key players in the risk management process — the board, which sets the risk appetite and provides strategic oversight for long-term value creation; executive management, which sets and executes risk management strategy; and the CAE, a resource for the board and management who provides assurance and insights independent from management.

In partnership with a global market research firm, The IIA has produced a unique report that captures the viewpoints from the boardroom, C-suite, and internal audit activity. It also introduces a Risk Stages Model — with stages ranging from Recognized to Maintained — that provide additional insight into developing risk management plans and strategies. In today's dynamic risk universe, risk management must effectively combine risk mitigation of potential negative outcomes with identification and prioritization of opportunities to enhance organizational value.

Through quantitative and qualitative surveys, *OnRisk 2020* not only identifies perspectives from each key player in the risk management process, it also maps how those views align. This additional insight into risk alignment provides vital data to measure how risks are understood and managed.

The mapping of how risk perspectives are aligned — or misaligned — provides deeper insight to support risk management planning in the coming year. It also sheds light into areas where misalignment can create weaknesses that can disrupt even the best risk strategies.

TOP RISKS FOR 2020 AND BEYOND

The 11 risks below were carefully selected from a vast assortment that are likely to affect organizations in 2020 and were vetted through in-depth interviews with board members, executive management, and CAEs.

CYBERSECURITY: The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

DATA PROTECTION: Beyond regulatory compliance, data privacy concerns are growing as investors and the general public demand greater control and increased security over personal data. This risk examines how organizations protect sensitive data in their care.

REGULATORY CHANGE: A variety of regulatory issues, from tariffs to new data privacy laws, drive interest in this risk. This risk examines the challenges organizations face in a dynamic and sometimes volatile regulatory environment.

BUSINESS CONTINUITY/CRISIS RESPONSE: Organizations face significant existential challenges, from cyber breaches and natural disasters to reputational scandals and succession planning. This risk examines organizations' abilities to prepare, react, respond, and recover.

DATA AND NEW TECHNOLOGY: Organizations face significant disruption driven by the accelerating pace of technology and the growing ease of mass data collection. Consider traditional versus born-digital business models. This risk examines organizations' abilities to leverage data and new technology to thrive in the fourth industrial revolution.

THIRD PARTY: Increasing reliance on third parties for services, especially around IT, demands greater oversight and improved processes. This risk examines organizations' abilities to select and monitor third-party contracts.

TALENT MANAGEMENT: Historically low unemployment, a growing gig economy, and the continuing impact of digitalization are redefining how work gets done. This risk examines challenges organizations face in identifying, acquiring, and retaining the right talent to achieve their objectives.

CULTURE: "The way things get done around here" has been at the core of a number of corporate scandals. This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive behavior.

BOARD INFORMATION: As regulators, investors, and the public demand stronger board oversight, boards place greater reliance on the information they are provided for decision-making. This risk examines whether boards are receiving complete, timely, transparent, accurate, and relevant information.

DATA ETHICS: Sophistication of the collection, analysis, and use of data is expanding exponentially, complicated by artificial intelligence. This risk examines organizational conduct and the potential associated reputational and financial damages for failure to establish proper data governance.

SUSTAINABILITY: The growth of environmental, social, and governance (ESG) awareness increasingly influences organizational decision-making. This risk examines organizations' abilities to establish strategies to address long-term sustainability issues.

KEY FINDINGS

The qualitative and quantitative interviews for *OnRisk 2020* elicited new insights about how the principal drivers of risk management interact, which risks pose the greatest challenges, and how alignment on risk management efforts impacts organizational success. Analysis of the results identified seven key findings that shed light not only into how risks are understood, but also how the ability to manage risk is perceived. In-depth examinations of these findings are found later in this report.

- **Boards are overconfident.** Boards consistently view the organization's capability to manage risks higher than executive management, evidence of a critical misalignment between what executive management believes and what is communicated to the board.
- **Boards generally perceive higher levels of maturity in risk management practices.** Board members' perceptions of risk knowledge and capability place them ahead of executive management and CAEs relative to risk maturity, therefore making them more likely to believe those risks are better managed.
- **"Acceptable misalignment"** on risk is a prevalent and dangerous mindset. A majority of respondents believe some misalignment on risk perception should be expected, with some viewing it as "healthy." While misalignment around individual knowledge of a risk may be acceptable based on varying roles, misalignment on the perception of the organization's capability to manage a risk is a serious concern.
- **Some industries are lagging in adopting systematic approaches to risk.** Healthcare, retail/wholesale, and public/municipal industries are lagging — sometimes significantly — in developing coordinated and consistent risk management processes.
- **Cybersecurity and Data and New Technology represent critical knowledge deficits.** Low reported knowledge and high relevance of these risks suggest risk management players should prioritize building knowledge in these two key risk areas.
- **Data and New Technology, Data Ethics, and Sustainability risks are expected to grow in relevance.** CAEs predict brisk growth in relevance for these three key risk areas in the next five years, identifying an opportunity for organizations to take a more proactive approach.
- **Talent Management** (and retention) are at the center of future concerns. Respondents recognize the importance of good talent and how people drive the success of a business — particularly when it comes to data and IT skills. An important shift is underway from an insufficient availability of resources to an inability to attract and retain talent with business-critical skills.

METHODOLOGY

The inaugural *OnRisk 2020* report is a significant step forward in collecting stakeholder perspectives on risk and risk management in support of good governance and organizational success. The combination of quantitative and qualitative research[1] provides a robust look at the top risks facing organizations in 2020 and allows for both objective data analysis and subjective insights based on responses from risk management leaders.

The qualitative survey is based on 90 in-depth interviews with professionals in North American boardrooms, C-suites, and internal audit functions. As part of the interviews, respondents were asked to evaluate 11 key risks on two scales: their personal awareness and knowledge of each risk and their perception of their organization's capability to address each risk. The ratings were based on a seven-point scale, with "Not at all knowledgeable" and "Extremely incapable" being the lowest ratings (1) and "Extremely knowledgeable" and "Extremely capable" being the highest ratings (7).

The combined responses for the two scales were then used to plot the position of each respondent group for each risk, where the X axis delineates perceived organizational capability, and the Y axis delineates personal knowledge of the risk (Figure 1). The values assigned for plotting purposes are derived as a percentage of respondents who scored their risk knowledge or their organization's risk capability as either 6 or 7 (top two ratings). Plotting the positions of all three respondent groups not only identifies how each group views each risk, it also graphically illustrates the degree of alignment among the groups.

The quantitative survey covers top risks as viewed by more than 600 internal audit leaders, primarily CAEs. The comprehensive survey also addressed organizational approaches to risk management, internal audit planning, resources, talent management, and internal audit's role in governance.

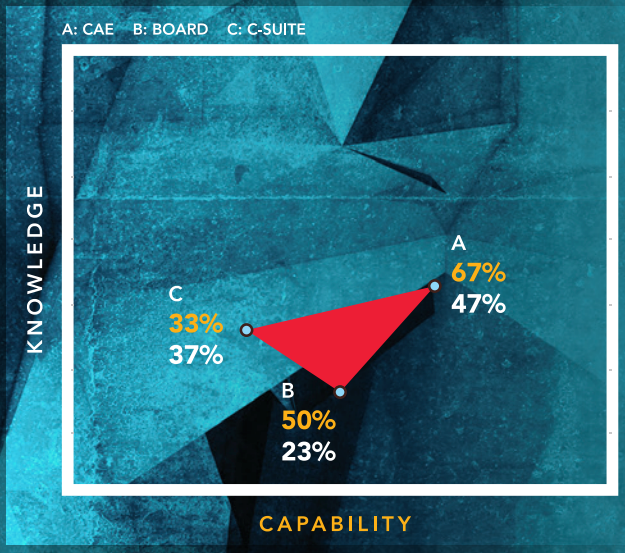


Figure 1: *Personal Knowledge/Organizational Capability Graph*

[1] *The quantitative survey of internal audit managers and CAEs and the qualitative interviews of board members, C-suite executives, and CAEs were conducted between June 4, 2019, and June 26, 2019.*

HOW TO USE THIS REPORT

Explanation of graphics

Based on in-depth interviews with 90 professionals, the personal knowledge and organizational capability of each of the three respondent groups were measured and plotted for each risk. Simple quadrant mapping (Figure 2) provides an effective and consistent tool to reflect those views.

The four quadrants of the graph correspond to the magnitude of each of the two measures. For example, responses with high ratings in knowledge and capability would be plotted in the top right quadrant. Conversely, responses with low ratings for knowledge and capability would be plotted in the lower left quadrant.

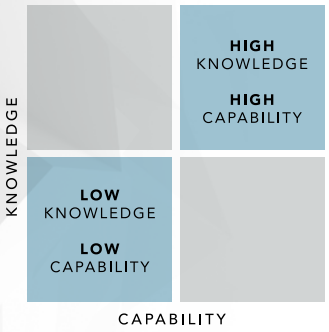


Figure 2:
Quadrant Graph

Position plotting

Positions for each of the three respondent groups are plotted on the quadrant map not only to identify the relative knowledge and capability on each risk, but also to graphically illustrate the degree of alignment among the groups that may exist. The resulting triangles — referred to simply as alignment triangles — provide a strong indicator of how well a risk is understood and managed. The size, shape, and location of each triangle also provides insights on what is driving any misalignment (see related sidebar).

Alignment Triangles:

What do they mean?

The alignment triangles created by plotting each respondent group's perspectives on each risk offer insights into how the risk is currently being managed. The shape of each triangle can provide valuable information, as well.

SHORT AND NARROW

Triangles with this basic shape suggest strong alignment on what each group knows about a risk, but significant disagreement by one respondent group about the organization's capability for addressing the risk.

TALL AND NARROW

Conversely, triangles with this basic shape suggest significant range of knowledge among respondent groups, but strong alignment on their views on organizational capability.

SHORT AND BROAD

This basic shape triangle suggests disagreement by more than one respondent group, with the most significant disagreement relating to the organization's capability to address the risk.

TALL AND BROAD

This basic shape suggests misalignment by more than one respondent group, with significant disagreement on both knowledge and capability.

SMALL AND SYMMETRICAL

This shape triangle suggests strong alignment of all three respondent groups on knowledge and capability. Depending on the location of the triangle, this could reflect a risk that is well understood and managed (top right quadrant) or one that is not well understood or managed (lower left quadrant).

LEVERAGING THE METHODOLOGY

Readers of *OnRisk 2020* should review and analyze the data for each of the 11 key risks that follow and are encouraged to conduct a similar analysis of the knowledge and capability perspectives among their own organization's board, executive management, and internal audit activity.

Comments from qualitative interview participants are interspersed throughout *OnRisk 2020* to offer a glimpse into not just *what* they think of each risk, but *how* they think about them. While these comments provide some insights, it is vital for every organization to have similar discussions about how each player in the risk management process understands risk and their perspectives on the organization's capacity to manage or leverage it.

A critical step in that analysis is to undertake a clear-eyed examination of how the three risk management roles currently operate and interact and the changes that should be contemplated in those roles to enhance the risk management process. For example, one of the key findings of *OnRisk 2020* is that boards appear to be more confident in their organizations' ability to manage risk than are executive management or CAEs. It is critical to examine and understand what is behind this skewed view, and to explore the changes needed to correct it.

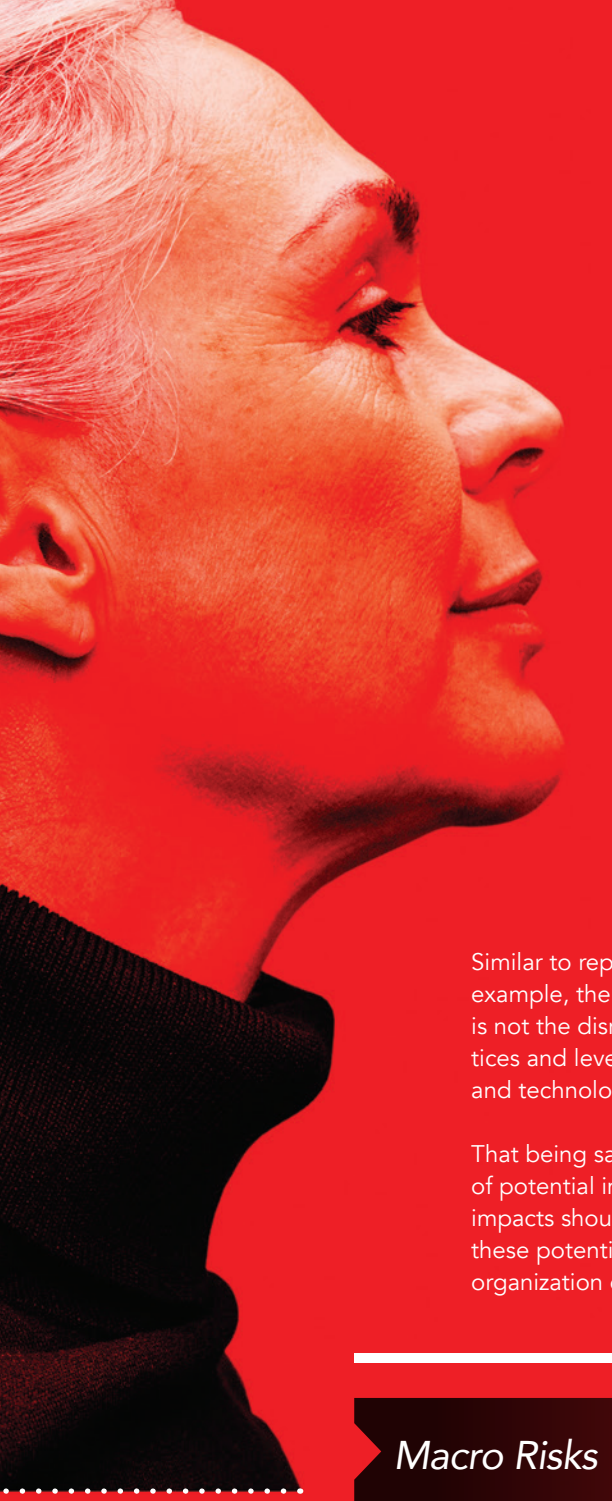
One reason for this misalignment may be the quality and completeness of information flowing to boards. Boards need information that is complete, accurate, and timely, and must establish proper oversight practices to ensure this.

This challenge is not unknown to boards. According to the National Association of Corporate Directors (NACD) report, *2019 Governance Outlook*, "Directors struggle to keep up with a rapidly evolving business landscape. For the second year in a row, NACD's public company governance survey found that a large majority of directors, almost 70 percent, report that their boards need to strengthen their understanding of the risks and opportunities affecting company performance."[2]

The cited public company governance survey also found boards are spending twice as much time reviewing information from management than from external sources, "revealing a heavy dependence on management views and analysis in fulfilling their oversight duties." What's more, more than half (53 percent) of directors indicated that the quality of information from management must improve, "suggesting the board needs better, not more, information from management."[3]

[2] *National Association of Corporate Directors and Partners, 2019 Governance Outlook: Projections on Emerging Board Matters (Arlington: NACD, 2018), 2.*

[3] *NACD, 2018-2019 NACD Public Company Governance Survey, (Arlington: NACD, 2018).*



UNDERSTANDING RISK

Reputation and Disruption in Risk Assessments

It is important to distinguish between a risk and the potential impact stemming from risk events. Reputational damage and business disruptions are often perceived as risks when in actuality they are consequences resulting from risk events. Boards, executive management, and internal audit can devote significant time and resources responding to and managing such consequences, yet may never understand or address the underlying risk, or root cause, that resulted in the event.

Reputational damage and business disruption may result from any number of risk events. For example, a ransomware cyberattack, where hackers block access to vital information, can cripple systems until a ransom is paid. If the attack is not properly managed, the organization will likely experience reputational damage. In this case, the reputational damage results from events related to cybersecurity, business continuity, and crisis response risks.

Similar to reputational damage, business disruption may result from a number of factors. For example, the proliferation of artificial intelligence challenges traditional business models. The risk is not the disruption itself, but the organization's ability to shift away from traditional manual practices and leverage data and new technologies to remain competitive in an increasingly complex and technology-driven environment.

That being said, boards, executive management, and internal auditors should be mindful of potential impacts related to business disruption and reputational damage. These potential impacts should be embedded in analyses of risks. Particular attention should be given to how these potential impacts may vary depending upon the industry and environment in which the organization operates.

Macro Risks

Macro risks may refer to economic or financial risks, political risks, or the impact of economic or financial variables on political risk. They may have widespread and significant influence on vital areas such as supply chains, short- and long-term planning, talent management and safety, and fraud and corruption.

The intertwined nature of macro risks may make them more complex than and just as dynamic as new or unknown risks. Examples include trade and tariff policy impacts on economic performance, and climate change leading to famine or natural disasters that can trigger geopolitical instability. What's more, macro risks can affect any organization, not just those that provide products and services to international markets. Indeed, organizations whose leaders believe they are immune to macro risks could end up underestimating or developing blind spots to key risks.

While *OnRisk 2020* is not designed to address macro risks, it is important to acknowledge their role in risk management strategies.

*Inherent **vs.** Residual*

Discussions about risk management can quickly become complex when strategy, competition, costs, and other factors are considered. This layer of complexity makes an already challenging discussion that much more difficult.

One way to simplify the discussion is to understand that risk may be measured on either an inherent or residual basis.

INHERENT RISK:
A theoretical description of what could go wrong if there were no controls or other risk management techniques. Most often applied to define the potential magnitude of risks and threats.

RESIDUAL RISK:
The risk remaining after management takes action to reduce the impact and likelihood of a risk event occurring, including control activities, in responding to a risk.[4]

These terms may seem like "auditor speak" to boards and executive management teams who are more likely to see risks in terms of impact and likelihood in their organization. Those viewpoints are typically associated with residual risk. In other words, boards and executive management are more likely to focus discussions on the risk that remains after risk management has reduced the impact and likelihood of a risk event occurring.

When weighing risk management resources, such as ERM and compliance programs, as well as internal audit activities, risk managers should consider the level of each risk to their organization. For example, fraud risk is well understood, and effective anti-fraud controls have been designed and tested over a long period of time. Most organizations have a strong understanding of the inherent risk fraud presents. However, the residual fraud risk depends on the controls in place in a particular organization and how effectively those controls are managed.

It is important for all players in the risk management process to understand inherent risk levels — the potential magnitude of risks and threats in the absence of risk management. This is especially applicable for atypical and emerging risks, where risk mitigation strategies are unlikely to have been developed.

[4] *Larry Sawyer et al., Sawyer's Guide for Internal Auditors, 6th ed. (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2012), 1: 186.*

THE STAGES OF RISK

In today's dynamic, technology-driven world, risks may emerge and impact organizations, sometimes at breakneck speeds. The risks discussed in this report are grouped into one of four stages as they relate to the potential impact on organizations and the actions organizations should take to address them — Recognize, Explore, Develop, and Maintain (Figure 4).

The Risk Stages Model (Figure 3) reflects how approaches to managing specific risks evolve within the organization. The colored graphic to the right shows that risk evolution on the same scale as the risk rankings — Knowledge and Capability.

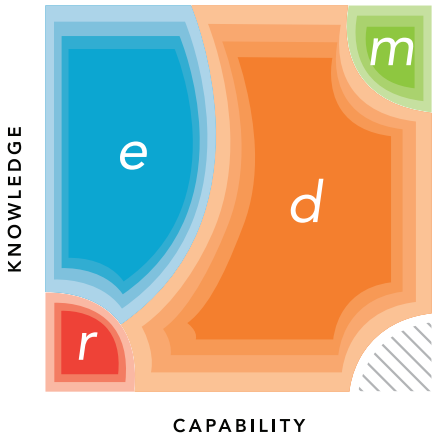


Figure 3: *Risk Stages Model* >
Risk stages are Recognize (r), Explore (e), Develop (d), Maintain (m).

Stages of Risk Explanation

RECOGNIZE

A risk is perceived as emerging and knowledge of the risk among stakeholders is low. Risk response strategies are not implemented or are not assumed to be effectively designed given the low understanding of the underlying risk. Monitoring processes have not been contemplated. Inherent risk levels are not well understood.

Knowledge – Low
Capability – Low

r

EXPLORE

Knowledge of the risk is growing among some but not all stakeholders. The risk may be perceived as emerging or dynamic. Risk response strategies have been contemplated, but have not been fully implemented. Monitoring processes have not been contemplated or are not implemented. Inherent risk levels are generally understood.

Knowledge – Mid to High
Capability – Low

e

DEVELOP

Risk knowledge is high, at least with management teams. Risk response strategies may be developed or in process of being implemented. Monitoring processes may be in contemplation, but are not likely to have been fully implemented. Residual risk is generally understood.

Knowledge – Low to High
Capability – Mid to High

d

MAINTAIN

Risk is well understood by all relevant stakeholders and is not perceived to be changing significantly. Risk response strategies, consistent with the perceived relevance of the risk, have been developed and implemented. Monitoring processes are utilized to ensure risk response strategies are operating effectively as designed. Residual risk levels are understood and believed to be at an acceptable level for the organization.

Knowledge – High
Capability – High

m

Figure 4: *Stages of Risk Explanation*

KEY FINDINGS EXPLAINED

The seven key findings introduced earlier are examined in depth in the following pages. As noted previously, the qualitative and quantitative interviews for *OnRisk 2020* were intended to elicit candid perspectives on the nature and understanding of risk management through the eyes of its three principal drivers. The analysis and examination of those views reveal important insights into interactions and alignment among respondents and informative conclusions about how those interactions and alignments impact risk management.

BOARD OVERCONFIDENCE

Boards are overconfident in their organizations' capability to address risks.

The qualitative survey responses and additional analysis uncovered a disturbing pattern. For every key risk, board members rated their organizations' capability for managing the risk higher than executive management did (Figure 5). This finding suggests boards may be failing to critically question information brought to them by executive management due to either receiving insufficient information or from limitations in their own competencies to understand and evaluate risks. The finding also suggests executive management may not be fully transparent with the board about risks and their own reservations about their organizations' ability to manage them.

Also notable is that executive management gives its highest ratings on risk management capability to Culture and Board Information, two areas often correlated with executive management performance.

The analysis explored whether boards' higher perceptions on capability were driven by low knowledge of the risks. The data did not support this hypothesis, further suggesting some level of breakdown in communication among the three parties (see Figures 7a and 7b in the section on acceptable misalignment).

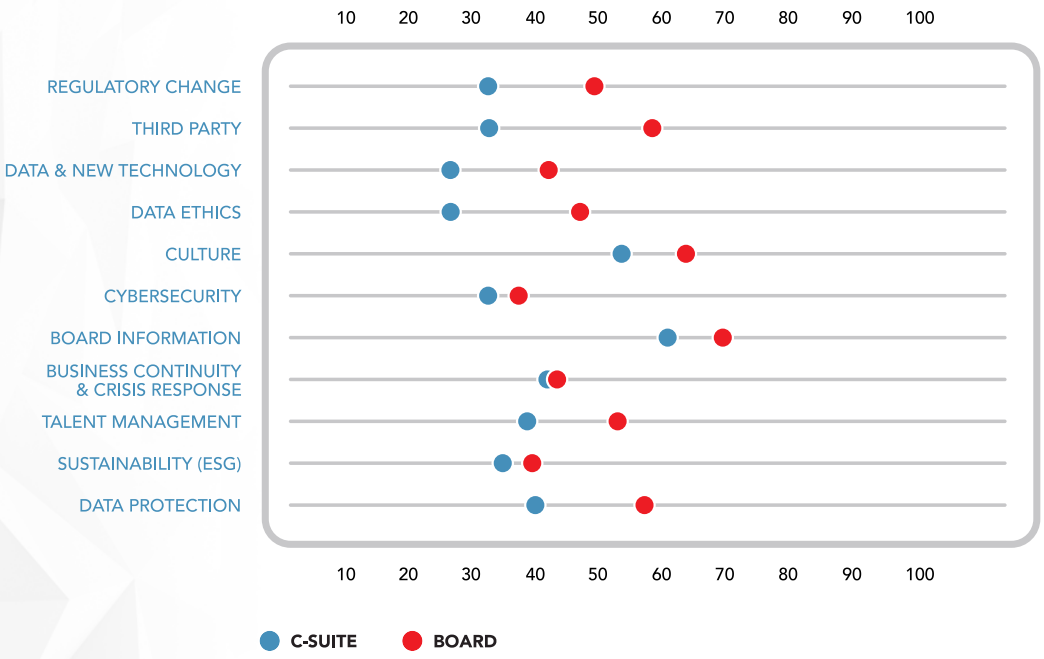


Figure 5: *Organizational Risk Capability: Board and C-suite Perceptions*

VIEWS MISALIGNED ON RISK MATURITY

Boards generally perceive higher levels of maturity in risk management practices.

Plotting the risk rankings on the Risk Stages Model (see section on risk stages, p. 11) confirms that boards are more optimistic in their organizations' abilities to manage risk, especially in comparison to executive management (Figure 6).

Boards consistently rate risk knowledge and capability in the range identified as *Develop*, where risk knowledge is high, risk management processes are being implemented, and residual risks are well understood.

Plotting risk rankings from executive management, meanwhile, reflects its more conservative view relative to the Risk Stages Model. Executive management ranks the majority of risks in the *Explore* stage, where knowledge of risk is growing, risks are perceived as emerging or dynamic, risk response strategies are contemplated but not fully implemented, and inherent risks level are generally understood.

CAEs' risk rankings are divided between the *Develop* and *Explore* stages, with the Data and New Technology risk rated in the *Recognize* stage, where risks are perceived as emerging, stakeholders have low knowledge of the risk, and inherent risk levels are not well understood.

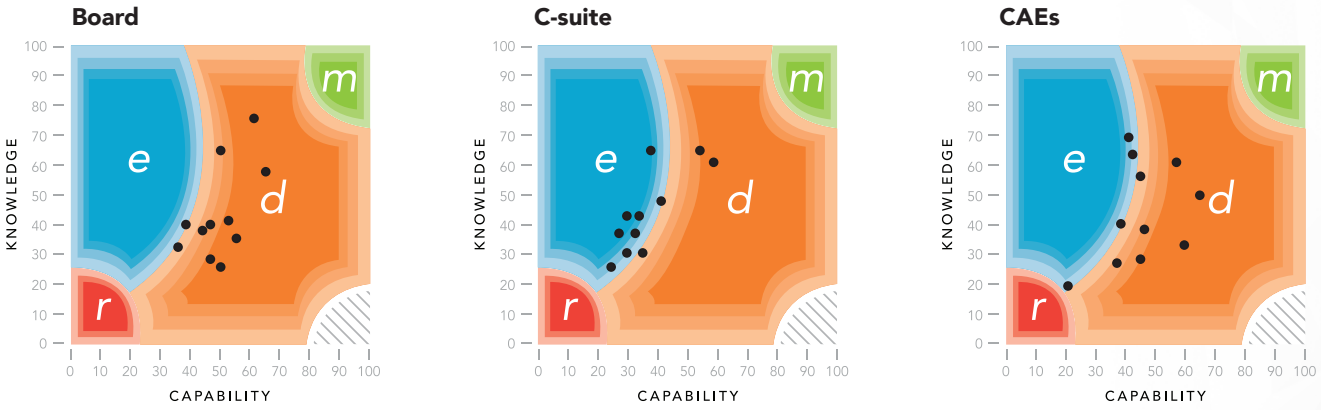


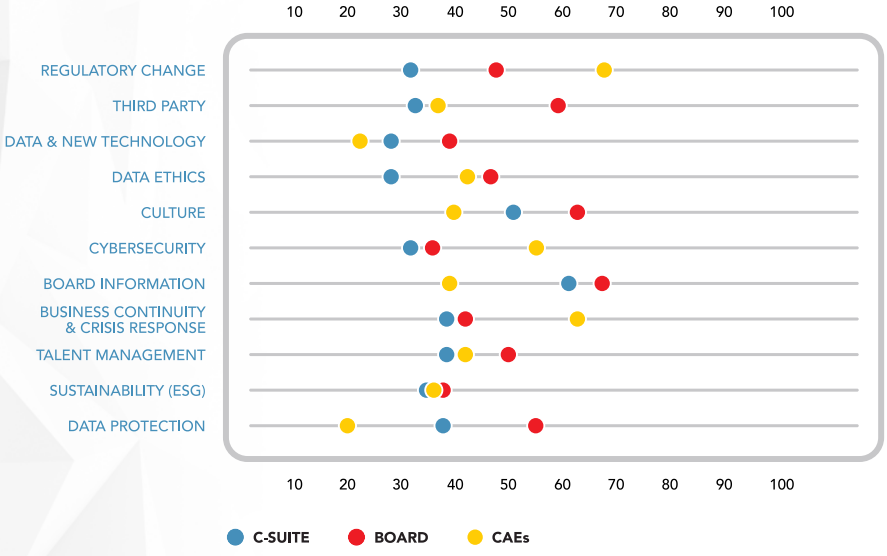
Figure 6: *Organizational Capability for 11 Risks Plotted on the Risk Stages Model*
Risk stages are Recognize (r), Explore (e), Develop (d), Maintain (m).

MISALIGNMENT DANGER

Acceptable misalignment is a prevalent and dangerous mindset.

Personal Knowledge

Organizational Capability



Figures 7a (top) and 7b (bottom): *Risk Knowledge and Capability: Alignment Among Board, C-suite, and CAEs*

A number of respondents downplayed the danger of misalignment among the parties. Indeed, many said that there was a "healthy" level of disconnect between CAEs, board members, and executive management. But the benefits of alignment (or negatives associated with misalignment) are often viewed through a lens biased by individual knowledge rather than a broader view incorporating organizational capability. Respondents differed in perspective, with most comments from CAEs centered on day-to-day operations (tactics), while comments from board members and executive management concentrated on risk strategy. The level at which a healthy disconnection becomes an unhealthy one was not addressed, leaving a dangerously nebulous gap that, in itself, is a risk.

The figures at left reflect how the three respondent groups rated their personal knowledge of the risk and their perception of the organization's capability to mitigate them. Note the tighter clustering for Personal Knowledge (Figure 7a) in comparison to the more widely spread ratings for Organizational Capability (Figure 7b). The disparity suggests that the comfort zone for acceptable misalignment expressed by the majority may be more benign for knowledge of the risk, where the variance is generally small, but the greater variance in perceived organizational capability logically raises a red flag.

" There is uncertainty and ambiguity in our company around risk."

– CAE, Business Services

RISK STRATEGY CONCERNS

Some industries lag in adopting systematic approaches to risk management.

While methods vary widely, a systematic approach to identifying, managing, and monitoring risks is critical to long-term value creation. Ideally, all organizations, regardless of sector, would adopt such approaches. While the type, likelihood, and impact of risks vary across industries, a holistic approach to risk management would undoubtedly benefit every organization.

Yet only about two-thirds (67 percent) of the CAEs surveyed report that their organizations have a systematic approach to identifying, managing and monitoring risk. Perhaps surprisingly, CAEs working in the healthcare, retail/wholesale, and public/municipal sectors rated their organizations' levels of risk discipline among the lowest when compared to their peers in other industries. (Figure 8). The low percentage of systematic risk management in these industries may indicate that individual business units are operating in risk silos. That is, the organizations may excel in managing certain risks, such as patient and drug safety in healthcare or natural disaster response in the public sector; however, the organizations are unable to routinely apply what they learn across the enterprise.

Additional analysis of responses based on organizational size (by revenue) found smaller organizations are as likely to be systematic as larger ones. This finding provides evidence to dispute the theory that systematic approaches to risk management correlate with resources and justifies serious concern about the reasons for the disparity among industries.

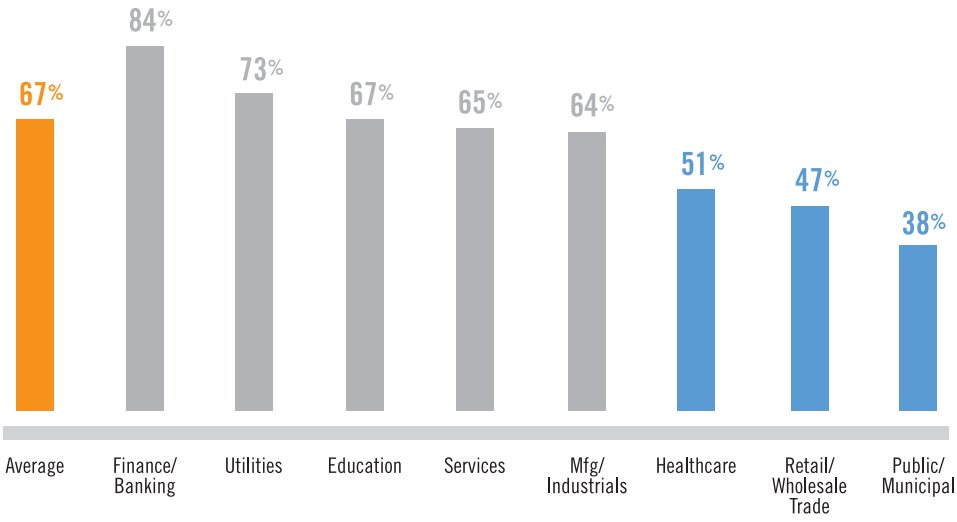


Figure 8: *Systematic Approach to Risk Industry Comparison*

INSUFFICIENT UNDERSTANDING OF SIGNIFICANT RISKS

Knowledge deficits in Cybersecurity, Data and New Technology can limit mitigation efforts.

Figure 9 reflects the key risks as they relate to Personal Knowledge and Organizational Relevance ratings among all respondents. This is a departure from the previous graphs of Knowledge and Capability ratings, but this comparison brings to life additional insights. The shaded area reflects those risks rated of highest relevance and lowest knowledge, thus pointing to where knowledge deficits exist. Respondents rated themselves relatively low on knowledge of Cybersecurity and Data and New Technology, yet rated the organizational relevance of those risks as high, which may make sense when the dynamic and complex nature of both risks are considered.

Data Protection and Business Continuity/Crisis Response fall just outside the shaded area, reflecting only slightly higher levels of knowledge and comparably high relevance ratings. Taken as a group, these four risks share a common element that contributes to knowledge deficits. All four involve outside entities constantly acting against the organization, whether hackers devising sinister new ways to attack or technology advancing faster than organizations can adapt and adopt.

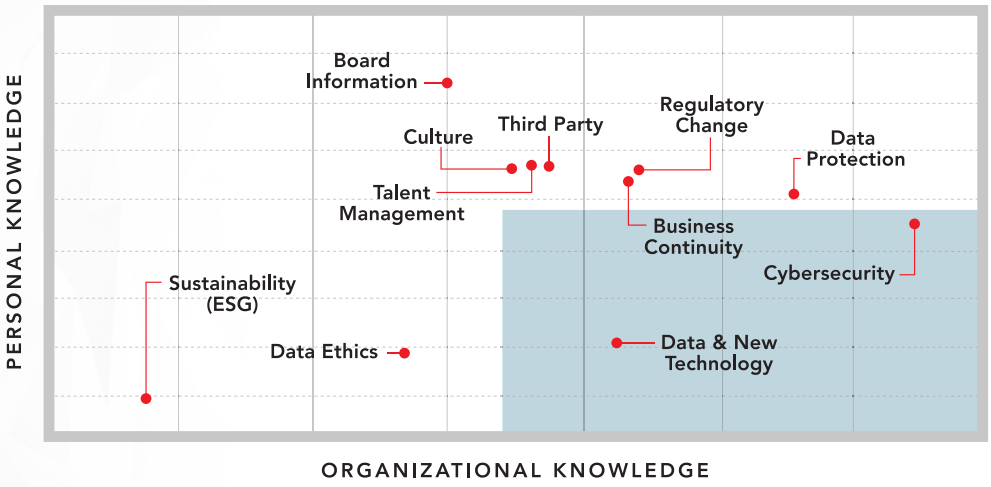


Figure 9: *Personal Risk Knowledge Risk Relevance Comparison*

THREE RISKS TO WATCH

Data and New Technology, Data Ethics, and ESG (Sustainability) will become more relevant risks.

The arrows in Figure 10 show predicted changes in risk relevance. Of the three risks discussed in this section, Data and New Technology was viewed as high in relevance at the time of the survey. However, as Figure 10 shows, respondents believe that the growth in the relevance of Data Ethics and Sustainability will greatly outpace the growth in relevance of the other risks over the next five years.

By beginning now to examine how they will address these risks, organizations may get ahead of the challenges associated with the risks and may discover opportunities to leverage them. For example, one of the greatest challenges in managing the risk related to Data and New Technology is assuring organizations are sufficiently flexible and prepared to adopt and adapt to technology that will support organizational growth and competitiveness. Such preparation involves building a corporate culture that is data- and cyber-savvy and readily embraces change.

In terms of Data Ethics, leaders in the boardroom and the C-suite must clearly establish organizational values, morals, and principles as guideposts to direct the collection, storage, management, and use of data while understanding the potentially significant consequences for failing to do so. Internal auditors should provide assurance that the organization is adhering to the established guideposts.

Data Ethics is closely tied to the third risk to watch, Sustainability (ESG). Organizations are under increasing pressure from activist investors, regulators, and others to show how long-term strategies reflect an understanding of resource limitations, impacts outside the organization, and overall commitment to good governance. Organizational leadership should take steps to expand its knowledge on how the organization is viewed and operates in its broader ecosystem.

RISK	CURRENT	FUTURE	CHANGE
CYBERSECURITY	86%	90%	+4 ↑
DATA PROTECTION	78%	85%	+7 ↑
REGULATORY CHANGE	66%	64%	-2 ↓
BUSINESS CONTINUITY	65%	67%	+2 ↑
DATA AND NEW TECHNOLOGY	64%	82%	+18 ↑
THIRD PARTY	60%	66%	+6 ↑
TALENT MANAGEMENT	58%	65%	+7 ↑
CULTURE	57%	58%	+1 ↑
BOARD INFORMATION	54%	51%	-3 ↓
DATA ETHICS	51%	66%	+15 ↑
SUSTAINABILITY (ESG)	30%	45%	+15 ↑

Figure 10: *Risk Relevance for 11 Risks*

FOCUS ON TALENT

Talent Management (and retention) are at the center of future concerns.

All three respondent groups recognize how people drive the success of the business — particularly when it comes to data and IT skills. With greater employee focus on social, political, and economic issues, and heightened competition to retain the best talent, respondents recognize company culture and employee satisfaction are increasingly important factors to success in the modern workplace. Most organizations know that filling seats with generic talent will not give them the competitive edge they need to thrive in today's rapidly changing risk landscape. Instead, organizations must find and develop individuals with the critical skills and expertise to keep up with evolving business practices and deliver innovation and growth.

Boards, executive management, and CAEs all believe their knowledge related to talent management risk is high. While the C-suite and CAE are fairly aligned in their assessments of the organizational capability to deal with such risk, board members have a slightly more optimistic perspective. This makes addressing board overconfidence that much more important.

Executive management and CAEs should collaborate to address the board's overconfidence about talent management so that all stakeholders become aligned around efforts to create formal talent management processes and diversity and inclusion initiatives to identify and attract employees with vital skills and manage the risk of losing top talent.

" Talent drives success … data integrity and cybersecurity are mitigated based on talent, which is based on culture. This will play a key role in the future."

– Board Member, Healthcare

" Management often creates culture and values from the top down … they know they need to take on better employees and solidify the hiring process because it's a big part of the business and will continue to be."

– CAE, Banking

CONCLUSION

The previous observations and findings were based on studied analyses of the data from the qualitative and quantitative surveys. What follows is an in-depth look at each of the key risks highlighted in the report. Carefully selected and validated by a cross-section of the three critical stakeholders, the risks covered here will impact all industries to varying degrees.

Each risk is examined based on a number of criteria, including relevance now and in the future, where the risk currently fits in the Risk Stages Model, and how the three respondent groups view the risk on the Personal Knowledge and Organizational Capability scales. These thought-provoking evaluations support the premise that alignment of the perspectives among the three respondents may significantly impact an organization's ability to manage risks and opportunities.

This section provides insightful gap analyses on risk perspectives, recommended actions for each stakeholder group aimed at improving alignment among them, and a benchmark against which to measure progress. Together, these comprise a valuable resource to which readers may refer throughout the year.

Note: The alignment triangle graphics for the following 11 risks are based on quantitative interviews of 90 combined respondents from boards, executive management, and CAEs. Each point of the triangle is labeled with a letter corresponding to each respondent group – A for CAEs, B for board members, and C for executive management. In addition, the corresponding percentage based on the top two answers for Personal Knowledge (blue) and Organizational Capability (red) are included in each label.

THE RISKS

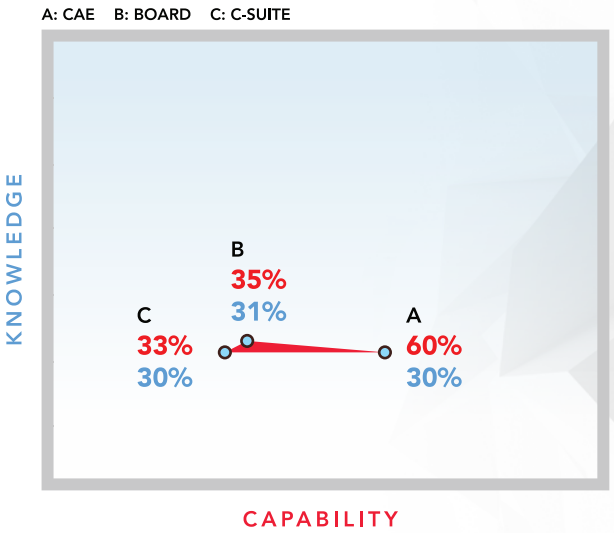
Managing risk is the art of building value while understanding what can be gained or lost from action or inaction, the foreseen or the unforeseen, the planned or the unplanned. Those who know what they don't know can ask questions. Those who don't know what they don't know are paralyzed.

CYBERSECURITY

The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

Gap Analysis:

Cybersecurity threats are a significant risk today and for the foreseeable future. The C-suite, board members, and CAEs are aligned in their perception that their knowledge of the topic is relatively low, which is likely attributable to the quick and ever-evolving nature of cyber risk. While senior leaders and board members are well aligned on their organizations' capability to address cybersecurity, CAEs appear to be overconfident. Considering their self-assessed knowledge of the topic is quite low, CAEs may be relying too readily on optimism expressed by CIOs and/or other providers of IT assurance and advice. With the C-suite's perception of capability appearing so much lower than that of the CAEs, the source of the incongruence is reason for concern.



Actions:

Board: Set expectations that management is continually providing briefings on emerging cybersecurity risks and action is being taken to address those risks. Hold management responsible and accountable for being transparent about vulnerabilities that require remediation or acceptance. Ensure that the internal audit activity is properly resourced to provide independent assurance on significant risks.

C-suite: Be transparent with the board and internal auditors about emerging cybersecurity risks and outstanding vulnerabilities. Leverage internal auditors as a resource to ensure that the controls created to mitigate or minimize cyber threats are designed and operating as intended.

CAE: Build trusting relationships with IT leadership to understand growing and emerging risks. Dedicate necessary resources to performing technical and non-technical reviews and consider hiring or co-sourcing specialty resources where necessary. Continually demonstrate professional skepticism regarding controls in place to mitigate cyber-related risks.

RISK STAGE

r

RISK RELEVANCE

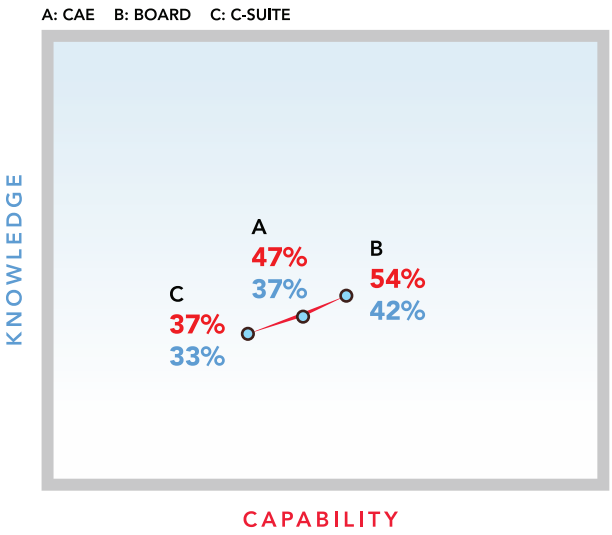
Source: See Figure 10

DATA PROTECTION

Beyond regulatory compliance, data privacy concerns are growing as investors and the general public demand greater control and increased security over personal data. This risk examines how organizations protect sensitive data in their care.

Gap Analysis:

Data protection is perceived as one of the highest priority risks and is expected to become more relevant, likely in response to expected increases in regulation, financial impact, and the potential for reputational damage. While board members, executive management, and CAEs all have some knowledge related to the risk, there may be opportunity for additional learning. Boards may have an overly optimistic perspective on their organizations' capability, perhaps due to insufficient exposure to information about the risks of failure to protect sensitive data and comply with increasingly complex data protection regulations. CAEs also appear to be more optimistic about organizational capability than senior leadership, which may result from an insufficient, or delayed, internal audit focus on this emerging and growing risk.



Actions:

Board: Use knowledge of the risk to ask pointed questions to the CAE and executive management around actions being taken to identify and protect the organization's most sensitive data, as well as comply with regulations.

C-suite and CAE: Provide regular updates to the board on limitations of the organization's ability to protect data and comply with regulations as well as communicating actions being taken to address the risks and limitations. Consider the use of outside subject matter experts to consult on current status and action items.

RISK STAGE

r

RISK RELEVANCE

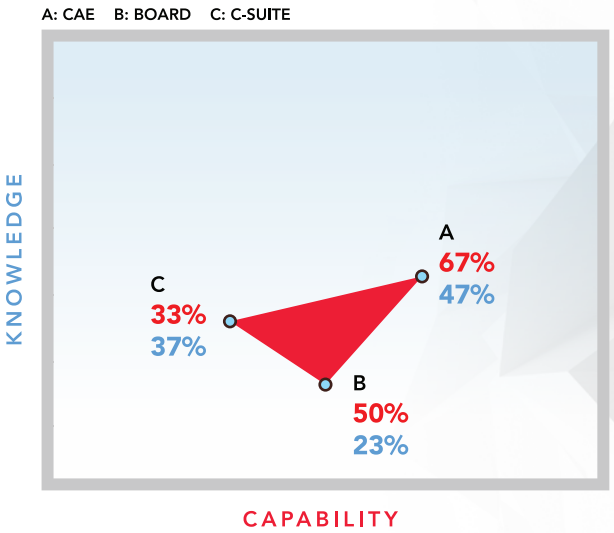
Source: See Figure 10

REGULATORY CHANGE

A variety of regulatory issues, from tariffs to new data privacy laws, drive interest in this risk. This risk examines the challenges organizations face in a dynamic, and sometimes volatile, regulatory environment.

Gap Analysis:

A significant misalignment exists among executive management, CAEs, and board members related to this risk. While opportunity exists to increase knowledge of regulatory change risk among all parties, this is particularly true of board members who may have a fiduciary responsibility to oversee their organizations' compliance activities. CAEs, and to a lesser extent board members, may be overly optimistic about their organizations' capabilities related to monitoring, adjusting to, and complying with regulations. This perceived capability gap should be of particular interest to those in industries, such as financial services, inherently subject to increasing and changing regulations.



Actions:

Board: Ensure adequate oversight processes have been established, particularly around mission-critical compliance issues. Set expectations that executive management regularly brief the board on new and proposed regulations relevant to the organization and that the CAE coordinates assurance coverage with providers of assurance over regulatory risks. Seek subject matter experts or other educational resources and opportunities to keep current on regulations and regulatory changes.

C-suite: Dedicate resources to continually monitor new and proposed regulatory changes. In highly regulated industries, ensure that monitoring activities are in place and properly resourced.

CAE: Dedicate audit resources to evaluating the organization's processes for monitoring and complying with regulatory change. Stay abreast of new and proposed regulatory changes, coordinate with those providing assurance over compliance risks, and be prepared to brief boards on potential impacts to operations.

RISK STAGE

d

RISK RELEVANCE

Source: See Figure 10

> *"**The company** overall needs to see the bigger picture and keep the bigger risks in the forefront of their mind. It's hard for departments to see beyond daily, weekly, and monthly functions."*

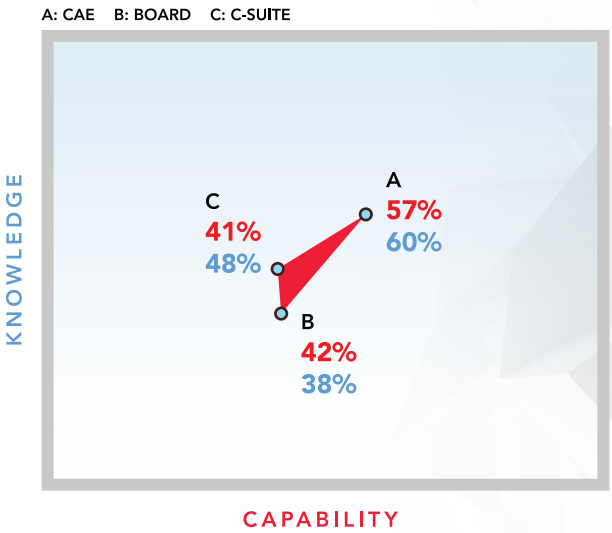
– Board Member, Tech

BUSINESS CONTINUITY AND CRISIS RESPONSE

Organizations face significant existential challenges, from cyber breaches and natural disasters to reputational scandals and succession planning. This risk examines organizations' abilities to prepare, react, respond, and recover.

Gap Analysis:

Here, CAEs are the outlier, viewing themselves as more knowledgeable than executive management and the board and reporting a more optimistic view of organizational capability to respond to and recover from crises and maintain business continuity. The C-suite and the board are aligned in their more conservative view of their organizations' capabilities. However, board members report notably less knowledge on the topic. The incongruity between CAEs' self-assessments and those of executive management and the board begs the question of whether CAEs are unrealistically confident, or rather, have more information to share with management and the board.



Actions:

Board: Set expectations of management to provide opportunities to enhance board members' understanding of related risks and their role in the processes. Further set expectations for a periodic overview of business continuity and crisis response plans, including risk assessments of scenarios that would most likely trigger the need to use those plans.

C-suite: Continually evaluate scenarios that would require business continuity and/or crisis response plans to be used. Work with the internal auditors in a consulting capacity to brainstorm risk scenarios and improve response plans. Test and update plans periodically and communicate scenarios and plans to the board.

CAE: Review organizational business continuity and crisis response plans, as well as results of scenarios conducted by management to test readiness for more likely events. Provide consulting services to help management improve its capability. Coordinate with other providers of assurance and consulting services to provide the board with coordinated assurance at the organizational level.

RISK STAGE

e

RISK RELEVANCE

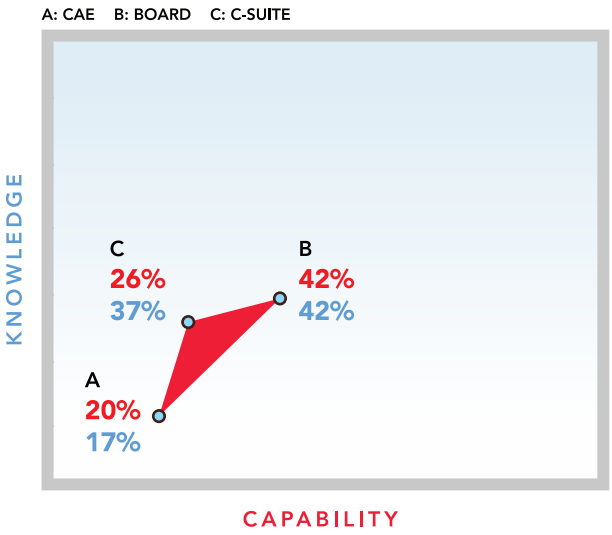
Source: See Figure 10

DATA AND NEW TECHNOLOGY

Organizations face significant disruption driven by the accelerating pace of technology and the growing ease of mass data collection. Consider traditional versus born-digital business models. This risk examines organizations' abilities to leverage data and new technology to thrive in the fourth industrial revolution.

Gap Analysis:

Although respondents ranked this risk among the top five in terms of current relevance and expect its relevance to grow more than any other on our list, CAEs rate their knowledge of the category quite low. Board members' greater perception of their organizations' capability to manage risks related to data and new technology may stem from positive information provided to them by management about the introduction of data and technology in the business without information about the underlying risks associated with those developments.



Actions:

Board: Set expectations of management that presentations demonstrating the use of data and new technology to drive the organizational strategy are balanced with information on potential negative impacts, including areas where the organization may be lagging in the use of data and new technology relative to the industry and/or competitors and the organization's ability to adapt to new technologies.

C-suite: Continue to explore new opportunities to leverage data and new technology to enhance organizational capability to meet strategic objectives. Provide balanced perspectives to the board with regards to organizational capability and challenges.

CAE: Dedicate resources to better understanding how the organization is leveraging data and technology in new ways. Ensure that risk universe and risk assessments take into account risks related to those uses of data and technology. Provide assurance on how data and new technology impact the collection, management, and protection of data.

RISK STAGE

r

RISK RELEVANCE

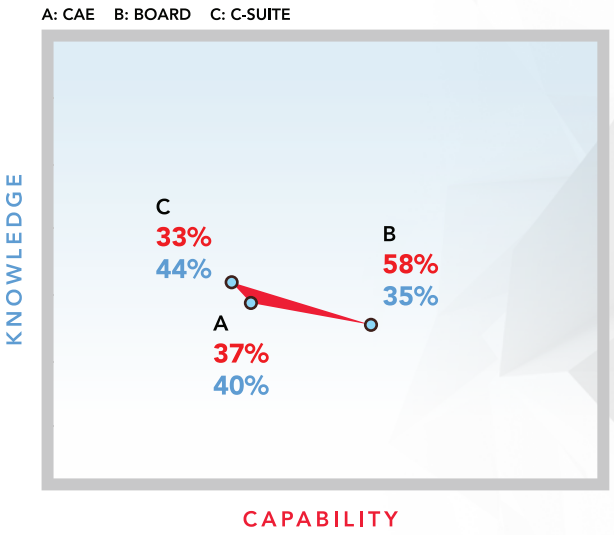
Source: See Figure 10

THIRD PARTY

Increasing reliance on third parties for services, especially around IT, demands greater oversight and improved processes. This risk examines organizations' abilities to select and monitor third-party contracts.

Gap Analysis:

As organizations continue to increase their outsourcing of business processes, risks related to third parties continue to grow. Executive management and CAEs appear to be relatively aligned regarding the capability related to the risk despite assessing their own knowledge of the category lower than their counterparts did. In contrast, board members appear much more optimistic about their organizations' abilities to engage and monitor third-party risk, despite having an admittedly lower knowledge of this risk. This misalignment may stem from boards having a limited understanding of where and how organizations depend on third parties. Further, this misalignment may be fueled by the dangerous misconception that outsourcing processes includes the transfer of risks related to those processes.



Actions:

Board: Ensure that management provides a holistic view of all significant third-party relationships, particularly those aligned with the organization's strategic objectives. Set expectations to receive briefings about any significant challenges that arise related to third-party relationships.

C-suite: Identify and prioritize all third-party relationships, giving particular attention to those that are large in value or those of any size that are key to the achievement of strategic objectives. Ensure that risks associated with each of the relationships are understood and accountability for managing the relationship has been appropriately assigned. Verify that "right-to-audit" provisions are included in all contracts.

CAE: Ensure that the internal audit activity has a holistic understanding of all significant third-party relationships. Give fair consideration to how these relationships fit into the organization's ecosystem of risks. Consider dedicating audit resources to evaluating overall third-party engagement and monitoring processes as well as processes around material third-party relationships.

RISK STAGE

e

RISK RELEVANCE

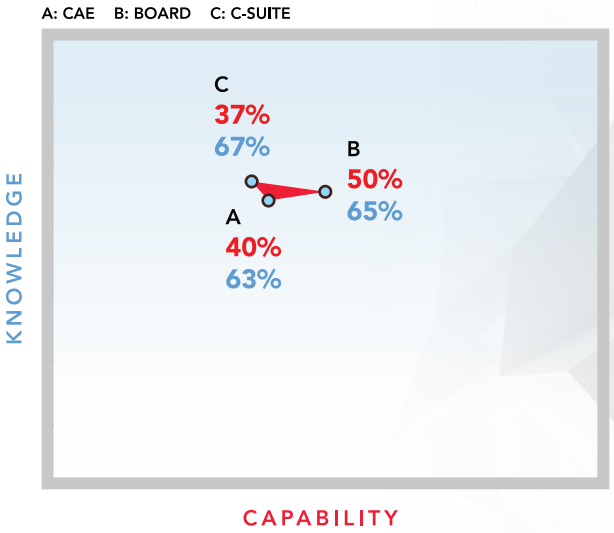
Source: See Figure 10

TALENT MANAGEMENT

Historically low unemployment, a growing gig economy, and the continuing impact of digitalization are redefining how work gets done. This risk examines challenges organizations face in identifying, acquiring, and retaining the right talent to achieve their objectives.

Gap Analysis:

Boards, CAEs, and members of the C-suite agree that they are relatively knowledgeable about risks related to talent management. The C-suite and CAE are fairly well aligned in their view of organizational capability to address talent management risks. Board members have a slightly more optimistic perspective, perhaps stemming from board members' primary focus on recruiting senior leadership talent. Executive management and CAEs may have a more holistic view and understand the potential talent management limitations at lower- to mid-levels, which largely remain outside the purview of the board.



Actions:

Board: Make periodic inquiries of senior leaders regarding talent management processes and risks related to lower- and mid-level employees.

C-suite and CAE: Continue to monitor emerging trends and associated risks related to talent management and provide updates to the board regarding initiatives taken and risks identified.

RISK STAGE

d

RISK RELEVANCE

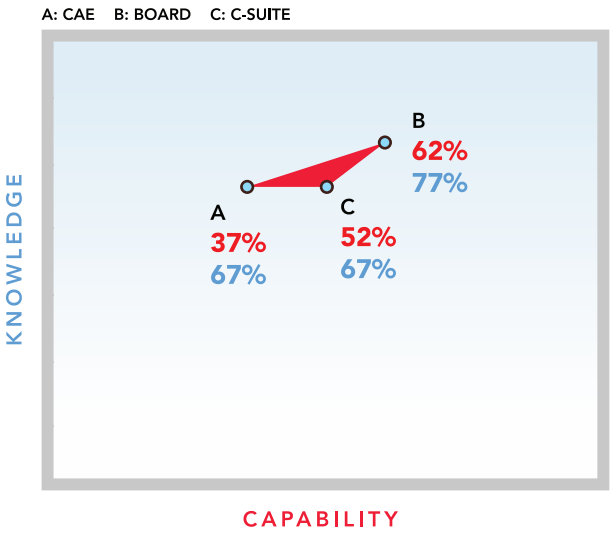
Source: See Figure 10

CULTURE

"The way things get done around here" has been at the core of a number of corporate scandals. This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive behavior.

Gap Analysis:

While senior leaders and CAEs are relatively confident in their knowledge around risks related to organizational culture, board members indicate they have a firm understanding of this risk, rating their knowledge of it higher than their knowledge of any other category. Board members are also more optimistic about their organizations' capability with regards to managing culture risk than are members of executive management, and CAEs are significantly less confident than either the board or the C-suite, with gaps of 25 points and 15 points, respectively.



Actions:

Board: Monitor actions taken by management to establish a positive culture within organizations, including reporting lines and safeguards, to allow for reporting of issues (whistleblowers). Seek insights from the internal audit activity for a perspective on culture independent from management.

C-suite: Set a positive tone at the top through communications and management actions. Establish management structures and reporting lines that allow for reporting of cultural issues. Recognize that incentives, both explicit and implicit, can drive unexpected and/or undesirable behaviors. Monitor and adjust accordingly.

CAE: Provide feedback directly to senior leaders when culture-related issues arise. Be prepared to answer questions from board members regarding organizational culture. Provide assurance that management structures and reporting lines are conducive to the ability to report culture-related issues.

RISK STAGE

m

RISK RELEVANCE

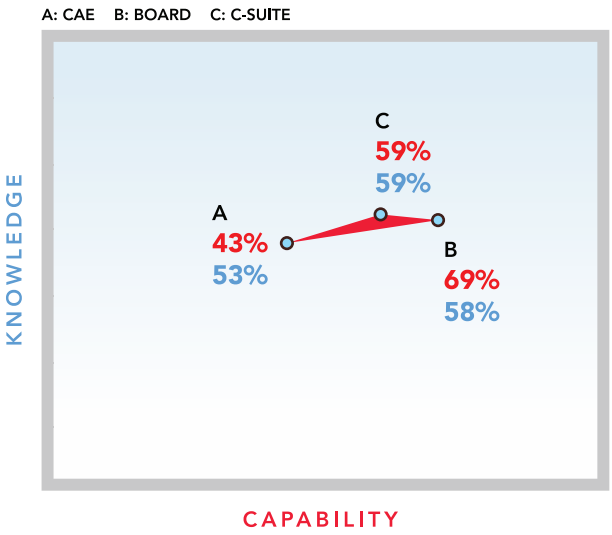
Source: See Figure 10

BOARD INFORMATION

As regulators, investors, and the public demand stronger board oversight, boards place greater reliance on the information they are provided for decision making. This risk examines whether boards are receiving complete, timely, transparent, accurate, and relevant information.

Gap Analysis:

CAEs, executive management, and board members all believe they are knowledgeable about risks related to the information that goes to the board. Senior leaders and board members display confidence in the capability of organizations to provide complete, accurate, and timely information to boards to perform their duties. CAEs are less confident in the capability of the organization to provide adequate information to the board. This may be attributable to the CAE believing that executive management is less than transparent. The CAE may lack knowledge about the information being provided to the board and/or have concerns about the quality of the information the board receives. In light of the findings on board overconfidence in risk management capability, misalignment in this area may be woefully underrepresented.



Actions:

Board: Apply professional skepticism in evaluating the information received from executive management. Solicit the CAE's opinion on the quality of information being provided. Hold management accountable when information appears to be inaccurate or is not provided timely.

C-suite: Provide complete, accurate, and timely information to the board, regardless of how it may be viewed by the board. Work with the CAE to provide assurance to the board regarding the quality of information provided.

CAE: Make inquiries of board members regarding their comfort level that information they are provided is complete, accurate, and timely. With board support, consider reviewing certain board materials, such as those involving mission-critical risks, to verify and communicate whether any information is incomplete or inaccurate.

RISK STAGE

d

RISK RELEVANCE

-3%

Source: See Figure 10

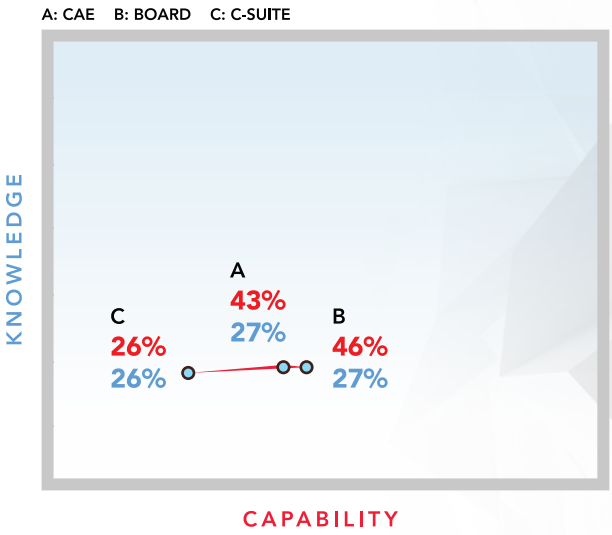
DATA ETHICS

Sophistication of the collection, analysis, and use of data is expanding exponentially, complicated by artificial intelligence. This risk examines organizational conduct and the potential associated reputational and financial damages for failure to establish proper data governance.

Gap Analysis:

While the concept of risk related to data ethics is relatively new, CAEs predict that its relevance will grow rapidly over the next five years. The board and CAEs are somewhat more optimistic about their organizations' capability to manage risks related to data ethics; however, all parties are aligned in their perspective that they lack significant knowledge on the risks. As the regulatory environment around data ethics evolves, all parties certainly must expand their knowledge of this risk.

.



Actions:

Board: Ensure that management has established and communicated expectations around how it will ethically collect, store, and use data consistent with the values and strategies established by the board.

C-suite: Establish expectations and limitations for how data can be used by the organization to ensure that data usage is consistent with the ethical values of the organization. Consider processes to monitor that organizational use of data is consistent with communicated expectations.

CAE: Take a leadership role in educating stakeholders, including the C-suite and board, on risks related to data ethics. Encourage management to develop guideposts that are aligned with the organization's risk tolerance related to the use of data. Provide assurance around adherence to established guideposts.

RISK STAGE

r

RISK RELEVANCE

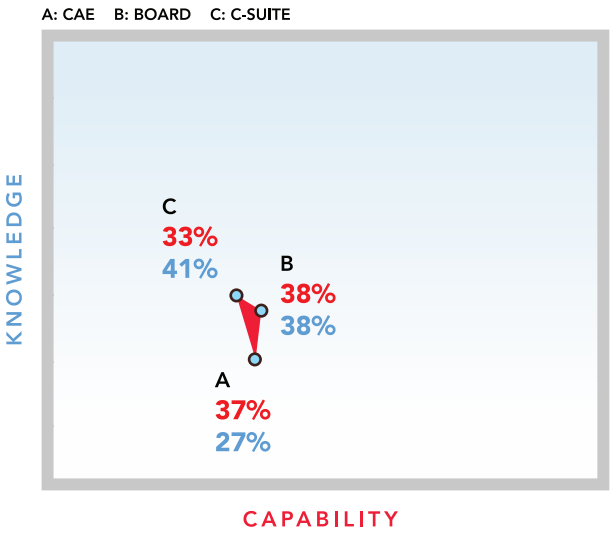
Source: See Figure 10

SUSTAINABILITY (ESG)

The growth of environmental, social, and governance (ESG) awareness increasingly influences organizational decision making. This risk examines organizations' abilities to establish strategies to address long-term sustainability issues.

Gap Analysis:

Executive management, board members, and CAEs assess their knowledge about the risks related to this relatively new and growing category as fairly limited, with senior management leading the parties in self-reported awareness and CAEs trailing 14 points behind them. The three groups are relatively aligned in their perception that their organizations' capabilities are low. This triangle depicts the organization's risk knowledge and capability moving from the *Recognize* stage into the *Explore* stage of the Risk Stages Model.



Actions:

Board: Seek additional sources of information regarding risks related to sustainability and board member responsibilities. Set expectations regarding management's responsibility to brief the board on emerging risks, organizational weaknesses, and actions being taken to remedy weaknesses.

C-suite: Seek expert advice regarding actions that management can take to reduce sustainability risks and identify best practices. Set a positive tone within the organization regarding the role it takes in providing sustainable value.

CAE: Take a leadership role by becoming more educated and sharing perspectives on risks related to sustainability across the organization. Seek feedback from the C-suite and board regarding internal audit's role in evaluating and recommending best practices related to sustainability.

RISK STAGE

e

RISK RELEVANCE

Source: See Figure 10

FIGURES

Figure 1 – Personal Knowledge/Organizational Capability Graph
Source: The Institute of Internal Auditors

Figure 2 – Quadrant Graph
Source: The Institute of Internal Auditors

Figure 3 – Risk Stages Model
Source: The Institute of Internal Auditors

Figure 4 – Stages of Risk Explanation
Source: The Institute of Internal Auditors

Figure 5 – Organizational Risk Capability: Board and C-suite Perceptions
Source: OnRisk 2020 qualitative interviews. Question: How capable is your company when it comes to handling each of the following risks? Combined percentage for scores of 6 or 7, with 7 being the highest level. *n* = 26 for board. *n* = 27 for executive management.

Figure 6 – Organizational Capability for 11 Risks Plotted on the Risk Stages Model
Source: OnRisk 2020 qualitative interviews. Question: How capable is your company when it comes to handling each of the following risks? Each of the plot points represents one of the 11 risks. Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. Risk stages are 1–Recognize (r), 2–Explore (e), 3–Develop (d), 4–Maintain (m). *n* = 26 for board. *n* = 27 for executive management. *n* = 30 for CAEs.

Figure 7a (top) and 7b (bottom) – Risk Knowledge and Capability: Alignment Among Board, C-suite, and CAEs
Source: OnRisk 2020 qualitative interviews. Questions: How knowledgeable are you about each of the following risks? How capable is your company when it comes to handling each of the following risks? Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. *n* = 26 for board. *n* = 27 for executive management. *n* = 30 for CAEs.

Figure 8 – Systematic Approach to Risk Industry Comparison
Source: OnRisk 2020 quantitative survey of CAEs. Question 8: Does your organization have a systematic approach to identifying and monitoring risks? The percentage of "yes" is reported. *n* = 630.

Figure 9 – Personal Risk Knowledge Risk Relevance Comparison
Source: OnRisk 2020 quantitative survey of CAEs. Question 1: How knowledgeable are you about each of the following risks? Question 2. How relevant are each of the following risks to your current organization? Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. *n* = 630.

Figure 10 – Risk Relevance for 11 Risks
Source: OnRisk 2020 quantitative survey of CAEs. Question 2: How relevant are each of the following risks to your current organization? Question 3: How relevant do you think each of the following risks will be in the next five years? Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. Those who chose not applicable/not sure for the risk rating were excluded from the calculation of the percentages. *n* = 630.

About The IIA
The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org

The Institute of Internal Auditors