ONRISK

A GUIDE TO UNDERSTANDING, ALIGNING, AND OPTIMIZING RISK

2021

TABLE OF CONTENTS

INTRODUCTION

Risk

The possibility of an event occurring that will have an impact on the achievement of objectives.

— IIA International Professional Practices Framework (IPPF)

Risk is part and parcel to modern economic theory. Indeed, nearly from the beginning of organized society, the push to recognize, leverage, and manage risk has driven humankind to excel. As social, business, and government institutions have become more complex, global, and entwined, mastering the art and science of risk management has become ever-more imperative — and elusive.

Last year, The Institute of Internal Auditors published *OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk*, which for the first time brought together essential perspectives of boards, management, and chief audit executives (CAEs) — the three key players in risk management. Through a series of interviews with members of all three groups, along with a survey of CAEs, OnRisk 2020 offered a unique and insightful examination of the interactions and views of those who most directly affect risk management. The inaugural guide was designed to improve alignment among these three risk management players by measuring their views on top risks, based on personal knowledge and organizational capability to manage those risks. OnRisk 2021 adds key players' views on organizational risk relevance as a factor in measuring alignment.

Observations gleaned this year show improved alignment on key risk knowledge and capability, but potential misalignment on how relevant some risks are viewed. The report also examines where organizations turn for assurance over risk management.

No examination of risk in 2020 would be complete without addressing the influence of COVID-19. Beyond the obvious fallout from shuttering the global economy for extended periods, response to the pandemic contributed to generally improved alignment among risk management players on business continuity, risk management, and communications. The pandemic also exposed the strengths and weaknesses of how organizations manage disruption. However, COVID-19's most influential long-term impact may be the marked acceleration of technology's positive and negative effects on cybersecurity, talent management, economic and political volatility, and disruptive innovation.

THE ONRISK APPROACH

The OnRisk approach uses an innovative methodology that uniquely brings together the perspectives of major contributors to organizational risk management. Alignment of these players' views on risk knowledge, capability, and relevance is a significant step toward achieving strong risk management in support of effective governance.

The methodology employed qualitative interviews of 30 board members, 30 C-suite executives, and 30 CAEs from 90 different organizations. Further support came from a quantitative survey of CAEs, which drew 348 responses.

The combination of qualitative and quantitative research provides robust data sets to examine top risks facing organizations and allows for both objective data analysis and subjective insights based on responses from risk management leaders. Further detail regarding the OnRisk methodology and how to use and leverage this report, as well as details explaining the Risk Stages Model developed in conjunction with OnRisk can be found in the appendices of this report.

TOP RISKS, 2021

The 11 risks were selected from a wide assortment that are likely to affect organizations in 2021 and vetted through in-depth interviews with board members, management, and CAEs. Some of the risks are unchanged from the inaugural OnRisk report, some descriptions have been updated, and other risks are new to the list. These risks should be relevant universally, regardless of an organization's size, industry, complexity, or type. However, this list does not cover all the significant risks in every organization; risks excluded from this analysis may have particular relevance — even significant relevance — to organizations, depending on their specific circumstances.

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.

THIRD PARTY: For an organization to be successful, it has to maintain healthy and fruitful relationships with its external business partnerships and vendors. This risk examines organizations' abilities to select and monitor third-party relationships.

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 feel confident that they are receiving complete, timely, transparent, accurate, and relevant information.

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.

DISRUPTIVE INNOVATION: We are in an era of innovative business models, fueled by disruptive technologies. This risk examines whether organizations are prepared to adapt to and/or capitalize on disruption.

ECONOMIC AND POLITICAL VOLATILITY: National elections, multinational trade agreements, new or extended protectionary tariffs, and uncertainty around timing of routine macroeconomic cycles all create volatility in the markets in which organizations operate. This risk examines the challenges and uncertainties organizations face in a dynamic and potentially volatile economic and political environment.

ORGANIZATIONAL GOVERNANCE: Governance encompasses all aspects of how an organization is directed and managed: the system of rules, practices, processes, and controls by which it operates. This risk examines whether organizations' governance assists or hinders achievement of objectives.

DATA GOVERNANCE: Organizations' reliance on data is expanding exponentially, complicated by advances in technology and changes in regulations. This risk examines organizations' overall strategic management of data: its collection, use, storage, security, and disposition.

TALENT MANAGEMENT: A growing gig economy, dynamic labor conditions, and the continuing impact of digitalization are redefining how work gets done. This risk examines challenges organizations face in identifying, acquiring, upskilling, 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 the desired behavior.

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

< BACK TO TOC

KEY OBSERVATIONS

The research for OnRisk 2021 provides a snapshot of how the principal drivers of risk management interact and which risks pose the greatest challenges to their organizations. Analyses of the data led to the identification of five key observations that shed light on how risks are understood and how an organization's ability to manage risk is perceived. In-depth examinations of these observations are found later in this report.

- **Business continuity and crisis management and cybersecurity are the top-rated risks for 2021.** Unprecedented challenges brought on by the COVID-19 pandemic as well as expanding reliance on technology and data drove these two risks to the top of the list. They often were paired as some cyber threats were heightened by the sudden relocation of employees to less secure work-from-home environments as well as an intense shift to e-commerce brought on by the pandemic response.

- **Two risks offer priorities for organizational improvement.** All respondents rated disruptive innovation and talent management among the most relevant risks. Yet, C-suite respondents ranked their personal knowledge and the organization's capabilities related to these risks among the lowest.

- **Management perceptions on risk relevance are generally not aligned with boards and CAEs.** Board members and CAEs were largely aligned on their perception of the relevance of risks included in OnRisk 2021. However, management relevance rankings were lower overall, with an especially large gap in the perception of governance and economic and political volatility. Indeed, the C-suite assigned higher relevance to operational risks such as talent management, culture, and business continuity.

- **Perceptions on capability to manage risks are more aligned.** This year, responses were more tightly clustered in ranking organizational ability to manage risk. The board overconfidence noted in last year's report appears to have eased. Responses to COVID-19, which focused in part on renewed risk assessments and more frequent communication and collaboration among risk management players, likely drove stronger alignment on organizational strengths and weaknesses.

- **Management sees organizational governance as a less relevant risk than do boards and internal audit.** The disparity in relevance rankings for organizational governance as a risk is significant and telling. Management's lower relevance ranking on this risk, combined with its higher rankings on personal knowledge and organizational capability, signal management overconfidence in this area and a disconnect from boards and CAEs.

KEY OBSERVATIONS EXPLAINED

The five key observations are examined in-depth in the following pages. As noted previously, the qualitative and quantitative surveys for OnRisk 2021 were intended to elicit candid perspectives on the nature and understanding of risk management through the eyes of its three principal drivers. The analyses of the data reveal essential insights into interactions and alignment among respondents, leading to enlightening conclusions about how those interactions and alignments impact risk management.

< BACK TO TOC

PANDEMIC RESPONSE DRIVES RELEVANCE RATINGS ON RISKS

Based on both qualitative and quantitative surveys, business continuity and crisis management and cybersecurity were the two most relevant risks among OnRisk respondents, which reflects 2020's unique context. The clear and present risk associated with keeping the doors open was rated right alongside the ever-expanding risk related to cyber threats (Figure 1).

Close to 9 in 10 (87%) board members ranked business continuity and crisis management as highly or extremely relevant, while more than 9 in 10 (93%) CAEs rated it as highly or extremely relevant. However, far fewer members of the C-suite identified it as such, with just more than 6 in 10 (63%) describing it as highly or extremely relevant. Generally, C-suite respondents assigned lower relevance rankings for all risks examined.

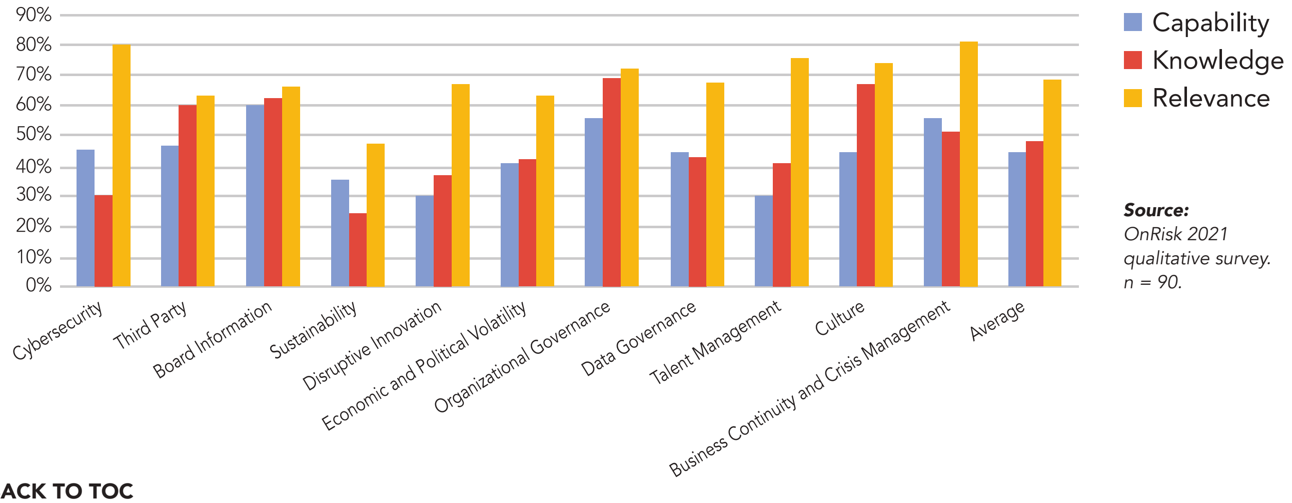
CAE rankings skewed the overall cybersecurity rating higher, with 90% rating it as highly or extremely relevant. However, board members put other risks ahead of cybersecurity, rating culture, talent management, board information, and organizational governance as more relevant. The C-suite gave cybersecurity its second highest rating overall, but a lower percentage rated it as highly or extremely relevant (73%).

> *"**COVID** definitely heightens the risk… showing financial documents on Zoom calls."*
>
> *–**Board***
> *Manufacturing/Utilities*

Board and C-suite respondents rate their level of personal knowledge lowest when it comes to cybersecurity. This may reflect continued uncertainty about a risk that is constantly evolving via technological advancement and related disruptive innovation. CAEs continue to be outliers in rating themselves significantly higher in knowledge about this risk. The three respondent groups were aligned and not particularly confident about organizational capability to manage cyber risks. On average, fewer than half of respondents (46%) rated their organizations as very or extremely capable.

COVID-19's influence on the relevance of these two risks is not surprising. The pandemic's existential threat to organizations, combined with the extreme measures taken to cope with the deadly virus, created new cyber vulnerabilities. For example, the newly ubiquitous work-from-home environment introduced the monumental task of enforcing cyber-safety protocols for entire offsite workforces. The perceived relevance and urgency of cyber-related risks was heightened further by changes to operations, mitigating the vulnerabilities of popular communications software, managing customer and vendor relationships strictly online, and internal audit's inability to perform on-site visits.

Figure 1: **ONRISK 2021 RISK RATINGS – ALL RESPONDENTS**



Source:
OnRisk 2021 qualitative survey. n = 90.

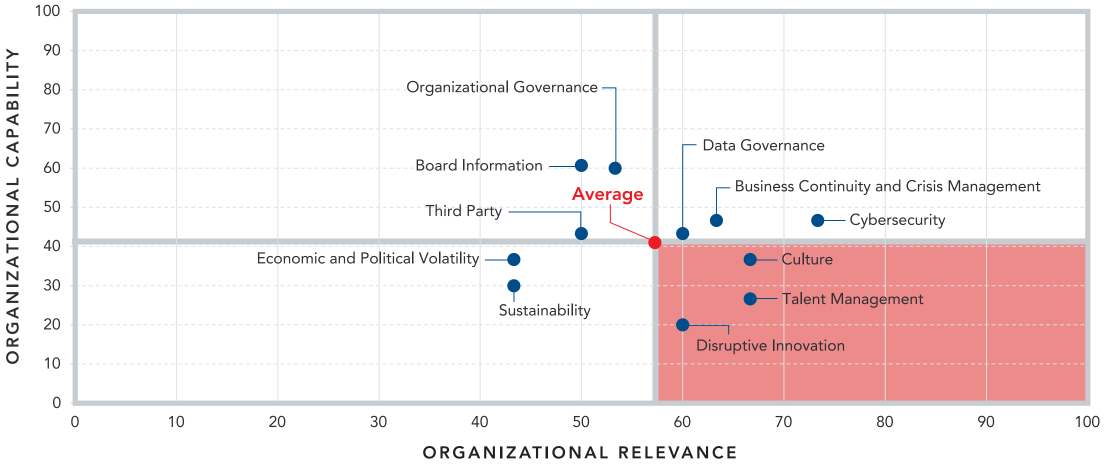
PRIORITIES FOR ORGANIZATIONAL IMPROVEMENT

Talent management, disruptive innovation emerge as clear areas for improvement.

Among all respondents, talent management and disruptive innovation emerged among the most relevant risks. Yet, C-suite respondents gave their lowest ratings to personal knowledge and organizational capabilities related to those risks. This discrepancy reveals two areas ripe for organizational improvement. The following comparison offers a simple but powerful insight into areas of potential risk management weakness. The X-axes in the graphics below (Figures 2 and 3) reflect relevance assigned by C-suite respondents to each of the 11 identified key risks. The corresponding Y-axes reflect management's rankings on either their personal knowledge or the organization's capabilities to manage each risk. The lower right quadrants of each graph represent areas of high significance but low knowledge or capability. The appearance of talent management and disruptive innovation in the lower right quadrants of both graphs (highlighted) visually depicts that these risk areas offer the greatest opportunities for improvement.

Figure 2:

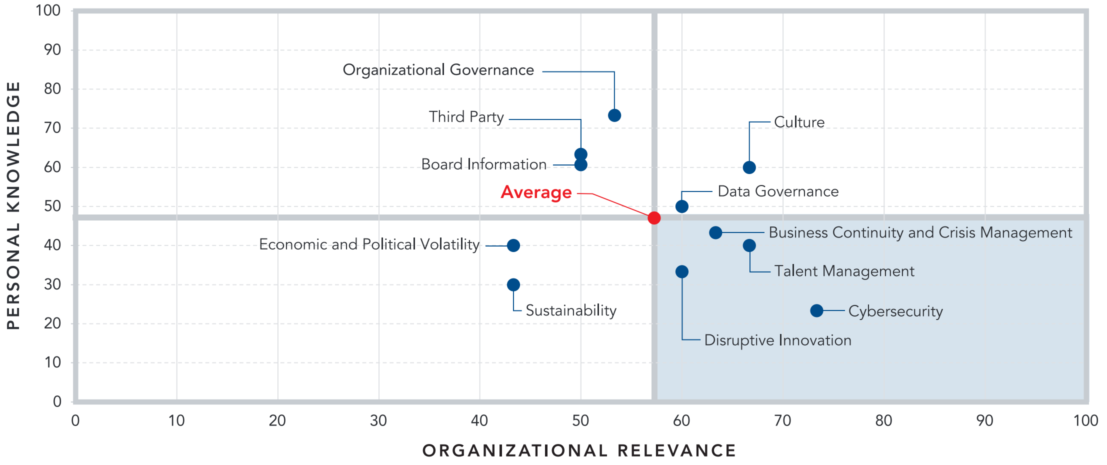
AREAS FOR IMPROVEMENT: C-SUITE



Source:
OnRisk 2021 qualitative survey.
n = 30.

Figure 3:

LEARNING OPPORTUNITIES: C-SUITE



Source:
OnRisk 2021 qualitative survey.
n = 30.

< BACK TO TOC

The timing of the surveys for the OnRisk 2021 report likely influenced the relevancy ratings for both talent management and disruptive innovation. COVID-19 pressed management into making difficult decisions on talent management. Similarly, management recognized and reacted to the potential impacts of continued disruptive innovation at a time when many organizations were particularly vulnerable to competition and felt pressure to quickly adopt new technology to support recovery. However, management's acknowledged lack of confidence in personal knowledge and organizational capabilities related to both areas cannot be dismissed.

TALENT MANAGEMENT

Identifying, hiring, and retaining top talent is a perennial and global challenge. Responding to COVID-19 added significant complexity to this risk category as organizations scrambled to react to lockdowns, related supply-chain and cash-flow disruptions, and an exodus of employees from traditional work sites. Pay cuts, furloughs, and workforce reductions followed as the pandemic's effects stretched from days to weeks to months.

This significant disruption to talent management, as well as its impact on morale, productivity, and workplace culture, will have both short- and long-term implications for organizations. Three areas offer evidence of its potential disruption.

1. *As organizations have quickly adopted new technologies to adapt to the pandemic, finding talent with new or modified skills has been critical. Organizations that responded most nimbly and effectively to this challenge may be more likely to emerge from the pandemic in a position of strength.*

2. *The work-from-home phenomenon has fundamentally changed how organizations recruit and manage talent. This accelerated evolution in the employment contract has positive and negative implications. While having a majority of the workforce operating in home settings posed significant immediate challenges in technology, cybersecurity, and logistics, it all but eliminated the limitation of geographic considerations when identifying and hiring the right talent. What's more, generous work-from-home options may become standard if organizations hope to compete for top talent in the future.*

3. *The "new normal" for employment has complicated the work-life balance equation, yielding multiple talent management implications related to paid time off, productivity, morale, and workplace culture.*

DISRUPTIVE INNOVATION

As organizations felt pressure to find new ways to operate effectively under pandemic-related restrictions, they accelerated the adoption of new technologies and abandoned cautious "wait-and-see" approaches to innovation, at least in the short term. This response bodes well for organizations that can make the leap successfully. However, the pandemic response exposed a potentially significant weakness: practically nothing will slow the pace of technological innovation and its related disruptions; yet, organizations appear ill-prepared to leverage or manage this risk.

Technology-driven assaults have dismantled legacy business models and built some of the 21st century's most recognizable brands — Uber, Amazon, Apple, Netflix. What's more, the greatest acceleration of disruption will likely come from combining powerful technological advances, such as SpaceX's Starlink project, which promises to bring low-cost internet services to remote areas of the world through a fleet of orbiting communication satellites. Organizations that embrace new technology and become leading-edge trailblazers will be best positioned to succeed. This will require 21st century management that not only understands and leverages disruptive innovation, but also nurtures it.

MANAGEMENT NOT ALIGNED ON RISK RELEVANCE

The introduction of relevance in OnRisk 2021 as a measure of overall risk management provides important insights into governance. Overall, there is strong alignment among all three risk management players on personal knowledge and organizational capabilities relative to the 11 key risks examined in the report. However, the average ratings for how relevant the risks are to organizations were better aligned between boards and CAEs (75% and 74%, respectively), than management's rating (57%) (Figure 4).

A detailed breakdown of relevance ratings further evidences that the board assigns more relevance to each risk than management does. A closer look also reveals which risks were most relevant to each group (Figure 5). For example, while talent management and culture appeared to be highly relevant to both the C-suite and the board, the board's relevance score exceeded that of management by about 20 points for each. Also, both groups rated business continuity and crisis management with high relevance, but boards rated the risk about 25 points higher than management did. The two groups were most closely aligned on the relevance of cybersecurity risk. However, the risk clearly topped the relevance list for C-suite respondents, while it was the sixth most relevant risk for board members.

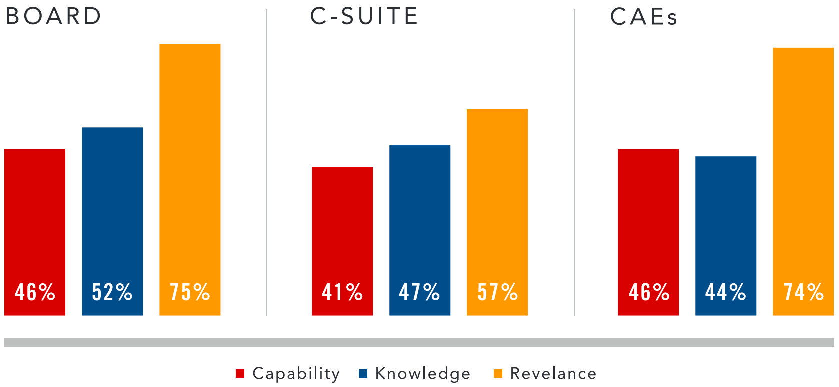


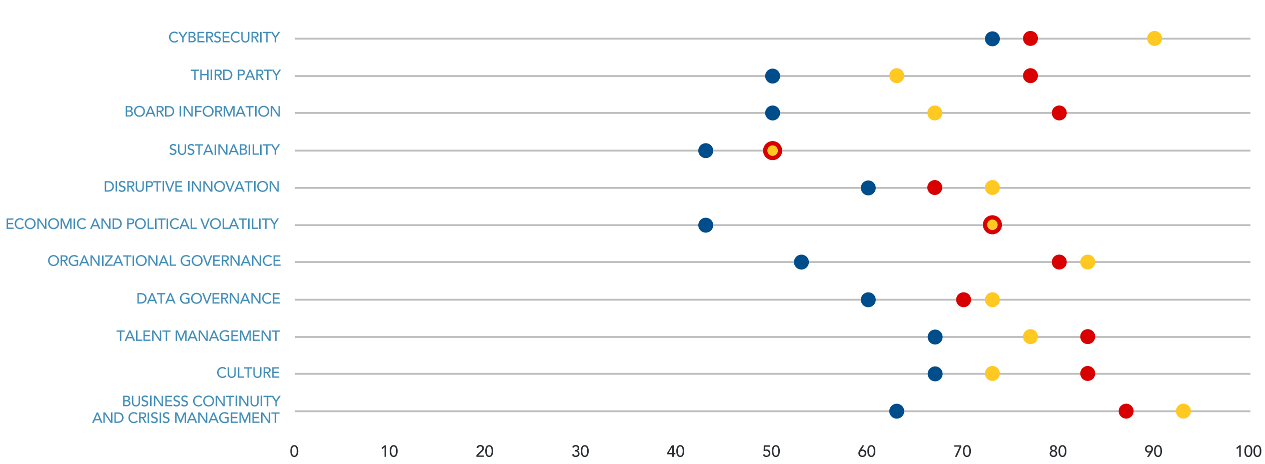
Figure 4:

AVERAGE RATINGS BY RESPONDENT GROUP

Source: *OnRisk 2021 qualitative survey. n = 90.*

Figure 5:

ORGANIZATIONAL RELEVANCE



Source: *OnRisk 2021 qualitative survey. n = 90.*

< BACK TO TOC

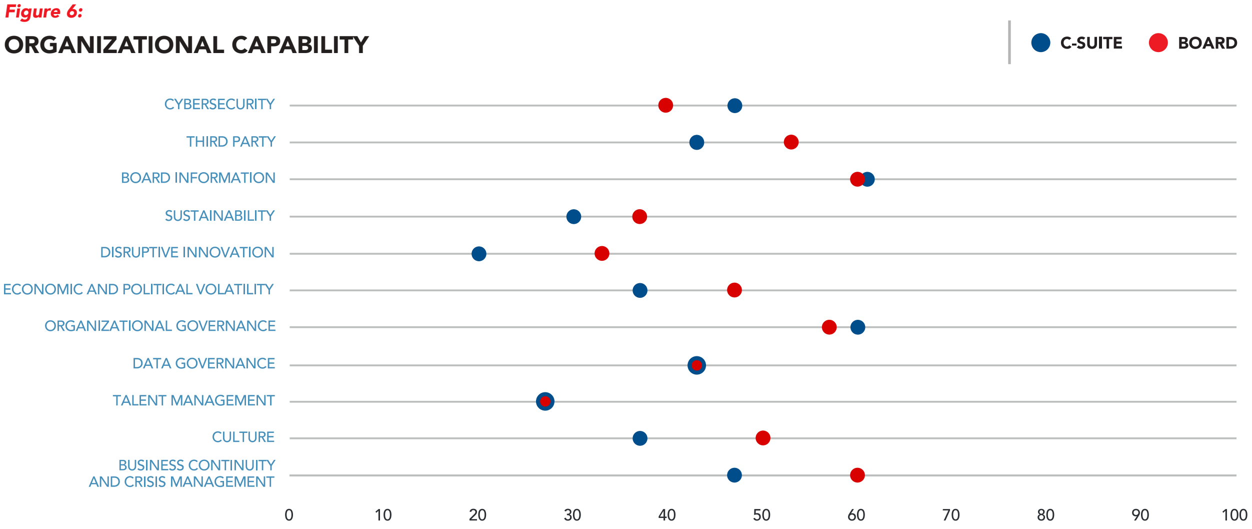
GREATER OVERALL ALIGNMENT ON CAPABILITY

Boards no longer outliers on ability to manage risks.

Perceptions on organizational capability to manage risks are more aligned compared to 2019, primarily due to lower rankings by boards this year in several risk areas (Figure 6), including talent management, board information, and data governance (previously data ethics, data protection, and data and new technology). This does not necessarily signal loss of confidence, but more likely a more realistic understanding of these risk areas. It is likely the pandemic prompted greater communication and fresh assessment of risks and capabilities. This is supported by board members rating their personal knowledge of risks on average higher this year compared to 2019.

Figure 6:

ORGANIZATIONAL CAPABILITY



Source: *OnRisk 2021 qualitative survey. n = 60.*

MISALIGNMENT ON ORGANIZATIONAL GOVERNANCE RISK

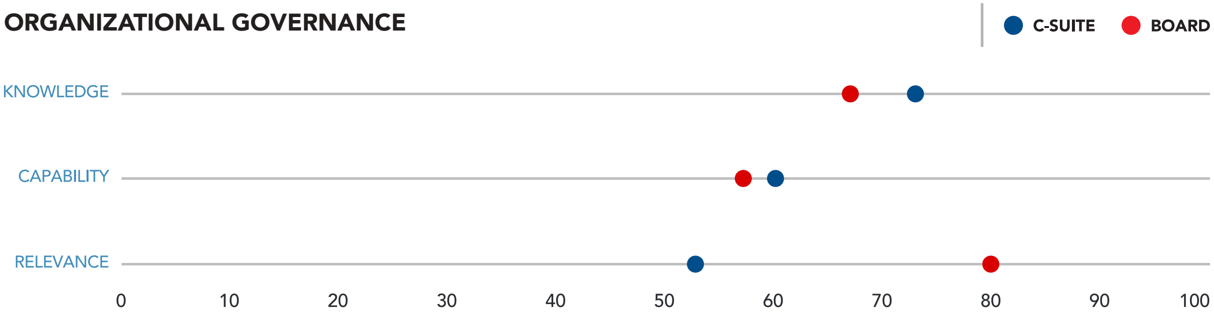
Management ranks knowledge and capability higher, relevance lower than do boards.

Management sees organizational governance risk substantially differently than do boards. C-suite respondents ranked their personal knowledge of the risk and the organization's ability to manage it slightly higher than boards did but ranked the risk much less relevant (Figure 7). This ranking pattern is illuminating.

Governance encompasses all aspects of how an organization is directed and managed, and it is commonly viewed as a useful barometer of management performance. Indeed, the strength of an organization's overall governance drives its ability to achieve its objectives.

Figure 7:

ORGANIZATIONAL GOVERNANCE



Source: *OnRisk 2021 qualitative survey. n = 60.*

C-suite respondents rated their personal knowledge and organizational capabilities to manage organizational governance risk higher than the board and internal audit. They also rated the relevance lower than both risk management partners.

The gap between the relevance rankings by management and the board should not be easily dismissed. Slightly more than 5 in 10 C-suite respondents ranked the relevance of organizational governance risk as highly or extremely relevant. In contrast, about 8 in 10 board respondents ranked it at those levels. This gap, about 25 points, signals a disconnect. This gap combined with management's higher ranking on personal knowledge and organizational capabilities reflect that management is either overconfident when it comes to organizational governance risk or simply unaware of the level of concern from board members in this area.

COVID

COVID-19'S IMPACT ON RISK MANAGEMENT

COVID-19 has been an unexpected, unwelcomed, and unstoppable test of risk management. Like no other event in recent memory, the pandemic is compelling organizations to examine risk management practices and performance in the struggle to excel, remain competitive, or simply keep the doors open.

What's more, no organization is being spared, and no two organizations are impacted in the same way. COVID-19 creates unique risk management challenges and opportunities for organizations large and small, public and private, established and start-up. It exposes the strengths and weaknesses of each organization's risk management and governance, as well as their agility and flexibility to manage through crisis. It stimulates leaders to imagine what success and competition will look like in a post-COVID-19 business environment that promises to be dramatically different.

Indeed, the pandemic's impact is evident in all aspects of our existence, from how it blurs the line between work and home to how it continues to redefine social interaction. Video chat platforms are the new boardroom and happy hour bistro. Face masks are killing lipstick sales but booming as fashion accessories. Amazon, UPS, and FedEx trucks invade neighborhoods as the 2020 version of ice cream trucks.

Data from the OnRisk 2021 surveys affirms some anticipated pandemic impacts, such as organizations focusing more on short-term, operational risks. It also tells of improved risk awareness and alignment among risk management players. But the most impactful revelation may be emerging signs of accelerating adoption of new technologies, a movement that promises to fundamentally change how work gets done. One C-suite respondent described this acceleration as "advancing the technology scale a few years in just a few months."

The short- and long-term impacts of this race to embrace disruptive innovation will be diverse and difficult to predict as implementation of technology can be fickle and frustrating even under the best circumstances. Transforming business processes, culture, and customer experiences at warp speed to meet the demands of a post-COVID-19 world will invariably lead to as many disastrous mistakes as happy accidents. It will almost certainly lead to new, as yet unforeseen risks, which organizations must be prepared to manage.

OnRisk 2021 data and additional research by The IIA bear out another moral from the pandemic. Organizations that invested in building strong internal relationships and technology pre-COVID-19 were best able to withstand the pandemic's challenges and uncertainties. This lesson is critical to organizations as they emerge from COVID-19's long shadow. Those that can successfully build and nurture alignment while advancing a clearly defined digital agenda will be best positioned to thrive in the pandemic's aftermath.

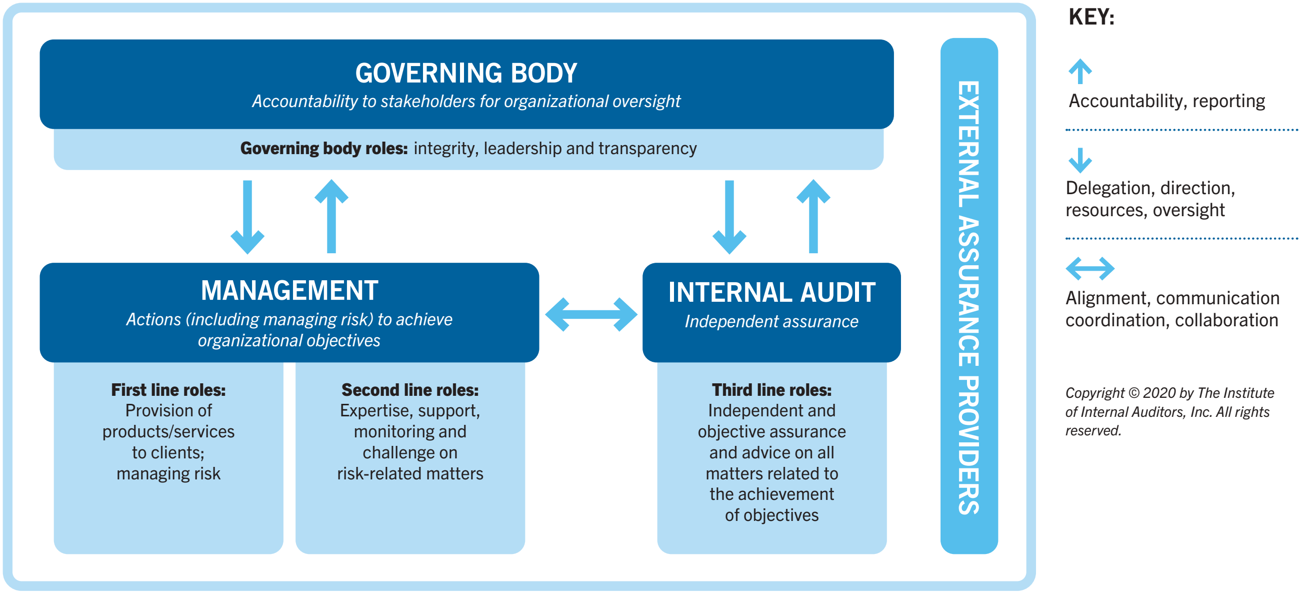
> *"It's amazing how [disruptive innovation] is driven by this virus. We're advancing the technology scale a few years in just a few months. Fueled disruptive innovation will impact virtually every business."*
>
> *– C-suite, Insurance*

RISK ASSURANCE AND THE THREE LINES MODEL

The Three Lines Model (Figure 8) is designed to help organizations identify structures and processes that facilitate strong governance and risk management. The new model, an update of the Three Lines of Defense, published by The IIA in July 2020, provides particular clarity to questions of assurance. The principles-based model identifies appropriate structures, processes, and roles that enable accountability from the governing body, actions (including managing risk) from management to achieve organizational objectives, and assurance from an independent and objective internal audit function.

Figure 8:

The IIA's Three Lines Model



GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
↑ Accountability, reporting
↓ Delegation, direction, resources, oversight
↔ Alignment, communication coordination, collaboration

Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

In clearly delineating roles to accomplish accountability, actions, and assurance, the model offers important guidance on assurance and the value of "improvement through rigorous inquiry and insightful communication" that an independent internal audit function provides.

Yet data from both qualitative and quantitative OnRisk 2021 surveys suggest that truly independent assurance is often lacking, and the sources of assurance are typically inconsistent. Leaders generally feel the level of assurance they are getting is satisfactory, regardless of where it comes from. However, this laissez-faire approach fails to address the value of an independent assurance assessment.

Internal audit coverage of key risks is considerable, but far from complete. CAEs report they provide assurance for each key risk examined in OnRisk 2021, but the percentage of those that do drops dramatically beyond cybersecurity, third party, business continuity and crisis management, and data governance (Figure 9). CAEs also report minimal assurance services in the areas of economic and political volatility and disruptive innovation, both of which were rated as higher in relevance by the group.

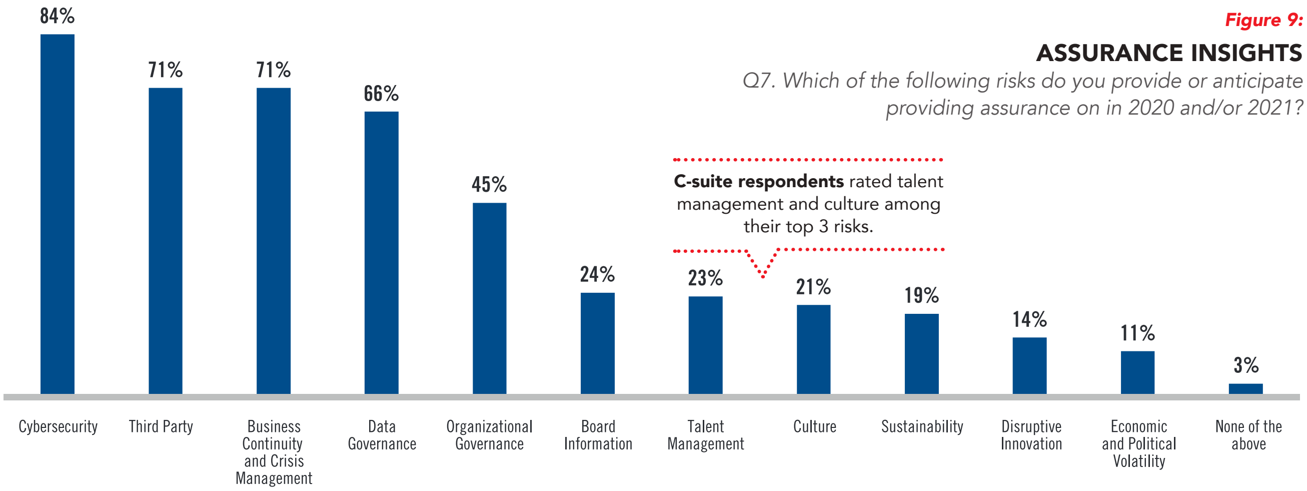
What's more, when compared to risk relevance rankings by the C-suite, internal audit provides minimal assurance on two of the C-suite's top three risks (see Figure 5 on page 11). This incomplete coverage may be due to limitations on resources, skills, or scope of work.

> *"Generally speaking, I'd say it's enough. We haven't had any major issues with it…so far, so good."*
>
> *– C-suite, Finance*

Figure 9:

ASSURANCE INSIGHTS

Q7. Which of the following risks do you provide or anticipate providing assurance on in 2020 and/or 2021?



Source: *OnRisk 2021 quantitative, n = 348., OnRisk 2021 qualitative, n = 30.*

Yet another factor influencing assurance is the use of internal audit as a consulting service. Organizations rely increasingly on internal audit's enterprisewide knowledge and perspectives on risk to provide advisory services. Unless sufficiently resourced, this practice can shift assets away from traditional assurance services. OnRisk 2021 respondents offered a variety of perspectives on internal audit's role within the organization. Some board and management respondents retain archaic views of internal auditors as accountants who provide little more than "tick-the-box" services or "police" who cannot be trusted as true business partners. Others point to organizational culture and weak internal audit leadership as contributing factors.

Figure 10:

TIPS ON ASSURANCE

OnRisk 2021 respondents offered a number of recommendations to improve assurance services and processes.

- Ensure internal audit's scope of work reflects the organization's assurance needs. Internal auditors must do more than just check boxes.
- Ensure internal audit reports directly to the board to create more transparency and improve information sharing.
- Ensure the audit team is well rounded and staffed with knowledgeable, confident, and assertive practitioners.
- Focus on obtaining high-quality assurance services from internal audit, not just consulting services.
- Clarify roles for internal and external auditors.

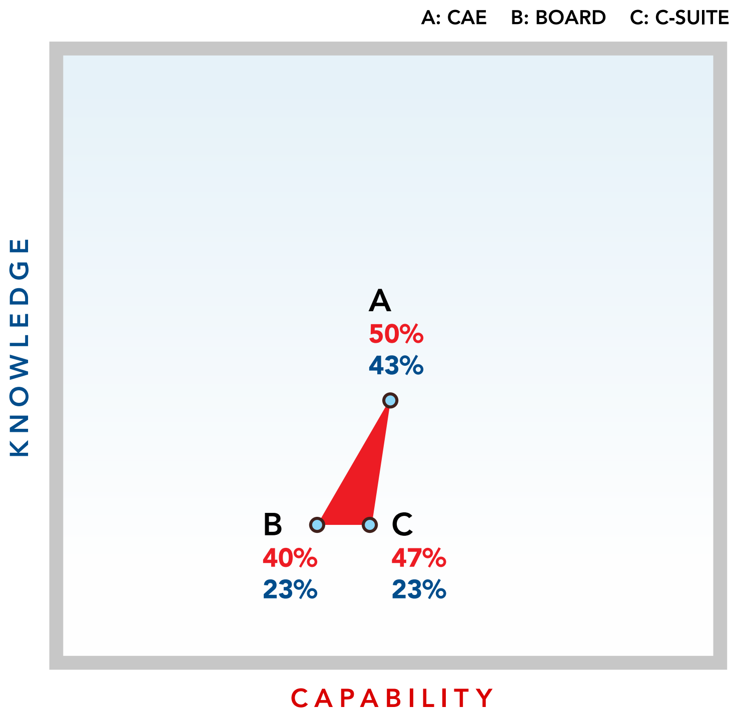
> *" I've seen a big difference in companies in terms of the role of IA. In some cases, they're a policeman, people don't really like them. In other cases they're a real business partner to improve controls and seen as a resource for well-trained employees."*
>
> *– Board, Retail/Grocery*

Source: *OnRisk 2021 qualitative survey. n = 90.*

THE RISKS

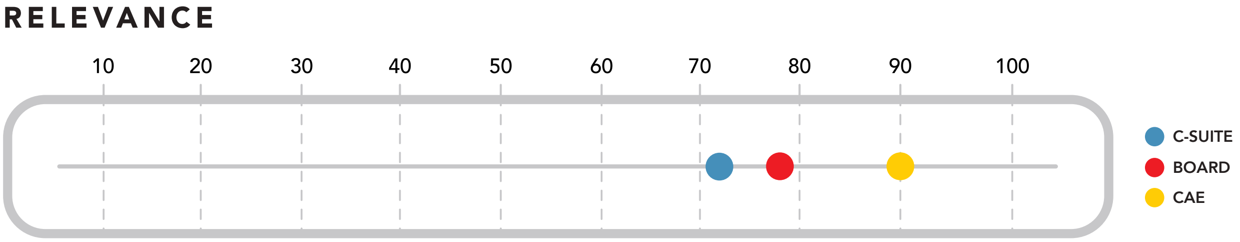
Managing risk is the art of building value by understanding what can be gained or lost from action or inaction, the foreseen or the unforeseen, the planned or the unplanned. Those who know what they don't know can ask questions. Those who don't know what they don't know are paralyzed. This section examines key observations related to individual risks; recommends actions to be taken by the board, management, and CAE to enhance risk management efforts; and identifies the developmental stage of each risk. More information about the methodology that supports these observations and the definitions that determine the stages of risk can be found in the appendices.

CYBERSECURITY



Analysis:

More members of management see cybersecurity as being highly relevant to their organizations than any other key risk. However, knowledge of this highly impactful risk remains particularly low among members of both the board and management. This low level of knowledge likely stems from the ever-evolving nature of cyber threats. All parties align in perceiving organizational capability to be quite low, especially when compared to the relevance of the risk.



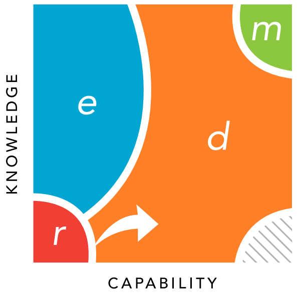
Actions:

C-suite: Dedicate necessary internal and/or external resources to consistently evaluate emerging cyber threats, get complete perspectives on current status, and provide transparent and thorough updates to the board.

Board: Ensure that appropriate time is allocated in meeting agendas for management, internal audit, and potentially outside subject matter experts to educate members of the board with a realistic perspective on emerging cyber threats, organizational efforts, and existing vulnerabilities.

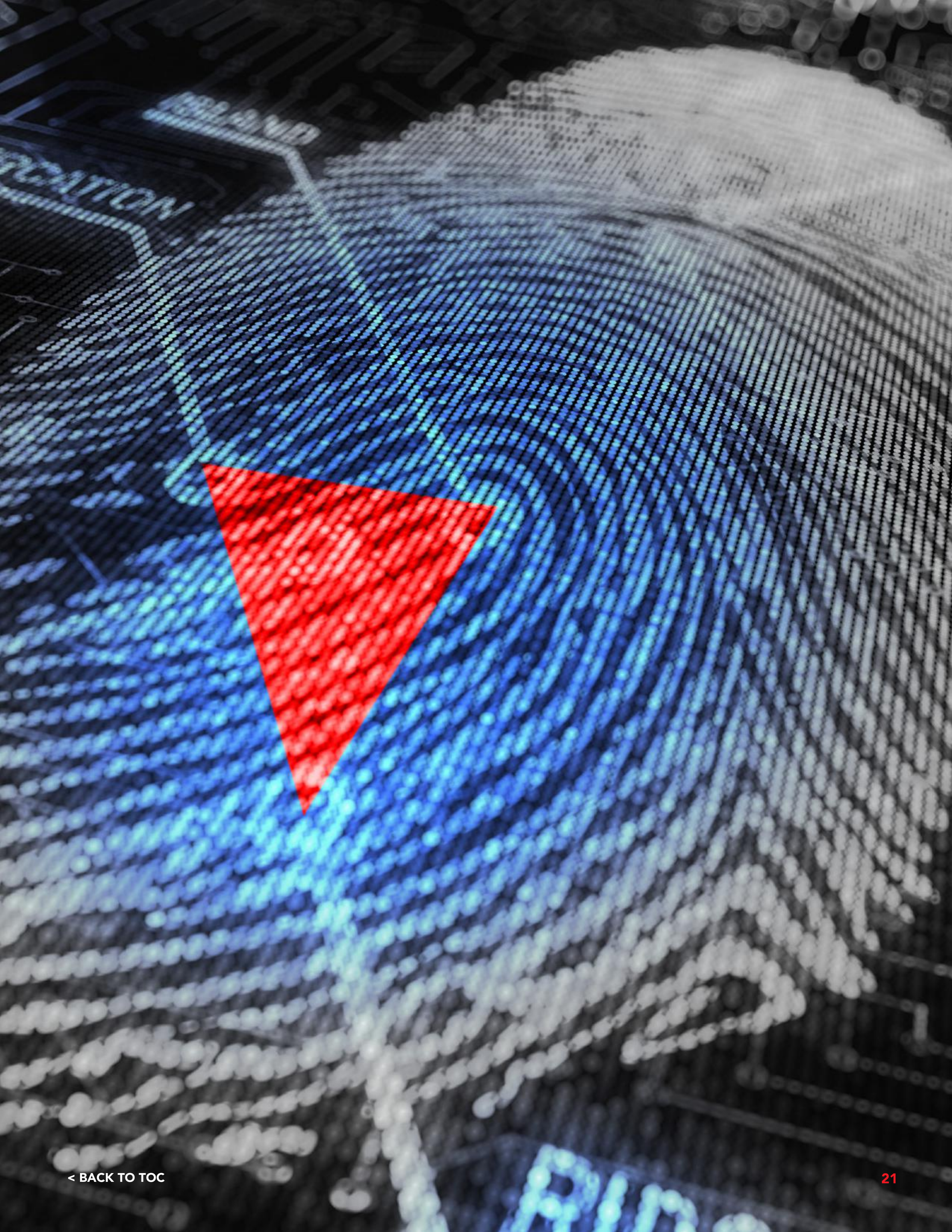
CAE: Identify opportunities to educate management and the board on emerging cyber risks and perform routine evaluations of all risk management functions related to cybersecurity.

RISK STAGE



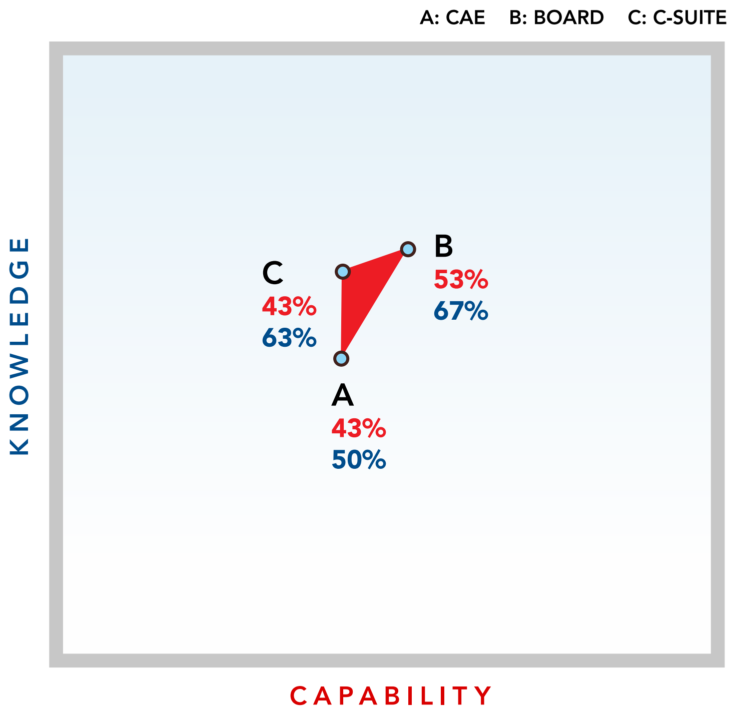
Moved from Recognize to Develop

< BACK TO TOC



CATION

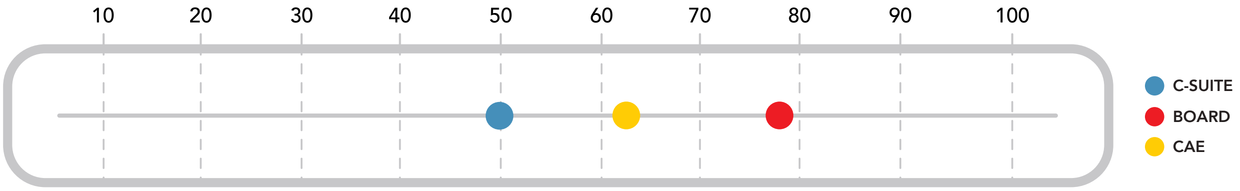
THIRD PARTY



Analysis:

CAEs and members of the C-suite are in agreement about organizational capability to manage third-party risk. However, board members are more confident. Surprisingly, fewer C-suite respondents than board members or CAEs consider third-party risks to be highly relevant.

RELEVANCE



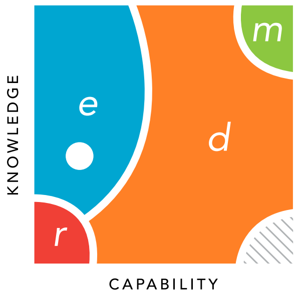
Actions:

C-suite: Management should ensure that a comprehensive list of third-party arrangements is maintained and that a risk-based approach is developed and followed to procure and monitor third-party relationships.

Board: Evaluate internal audit plans to ensure that adequate resources are allocated to third-party risks. Set expectations that management periodically communicates the status of key third-party relationships.

CAE: Periodically and regularly evaluate management processes related to establishing and monitoring third-party relationships. Consider including engagements to review third-party relationships that are operationally or strategically important to the organization.

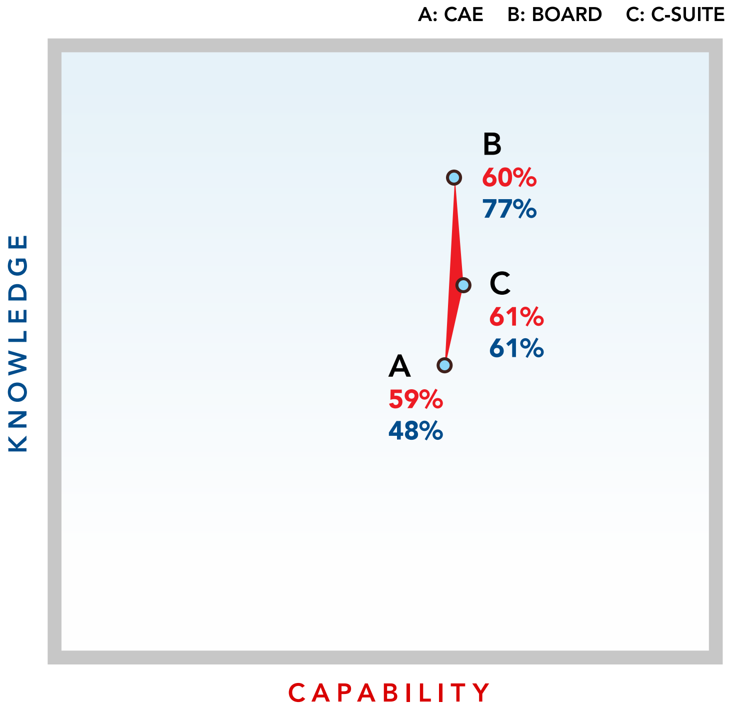
RISK STAGE



Remained in Explore

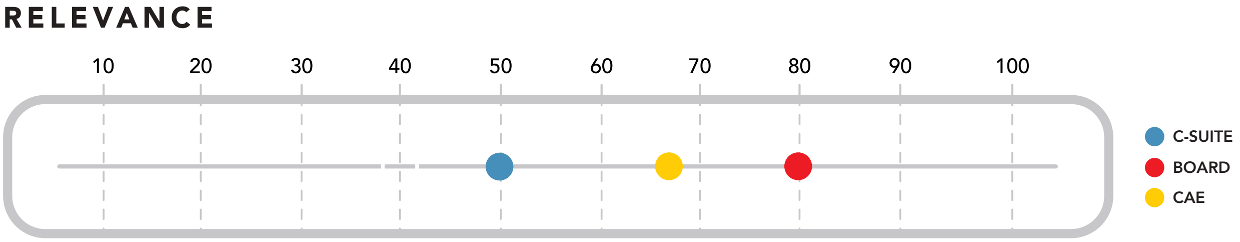
< BACK TO TOC

BOARD INFORMATION



Analysis:

All parties are aligned regarding organizational capability to manage risks related to the quality of information provided to boards. Not surprisingly, board members rate themselves as more knowledgeable about this risk category.



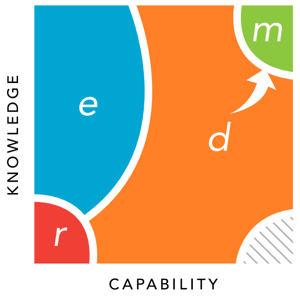
Actions:

C-suite: Enhance communication to ensure transparent, complete, and timely information is provided to the board, particularly regarding key risks.

Board: Set expectations with management and CAEs about the level of information to be provided. Be willing to communicate if excessive amounts of information overwhelm clear messaging. Seek independent assurance related to the quality of information provided.

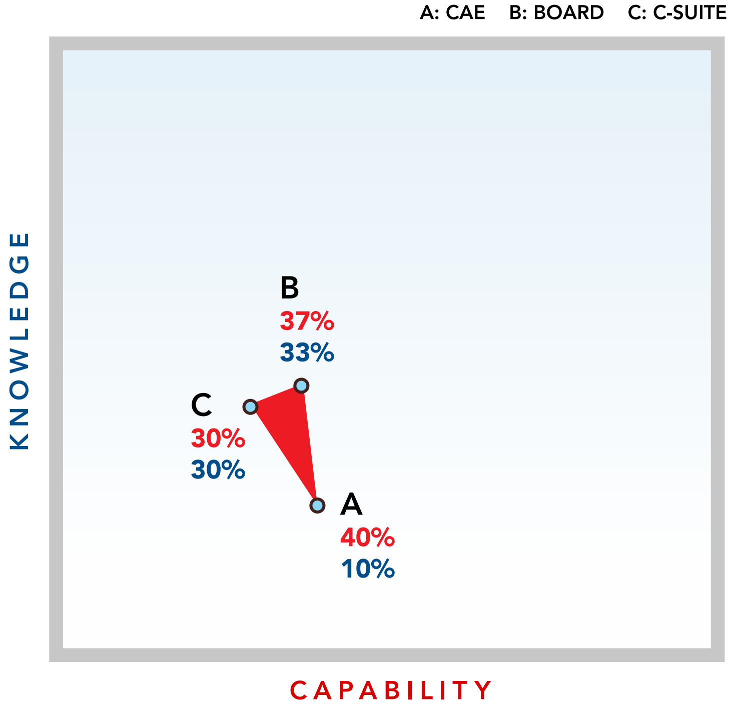
CAE: Evaluate information provided to the board, noting inconsistencies or omissions. Inquire with board members about the quality of information being provided, and be willing to contribute an objective assessment.

RISK STAGE



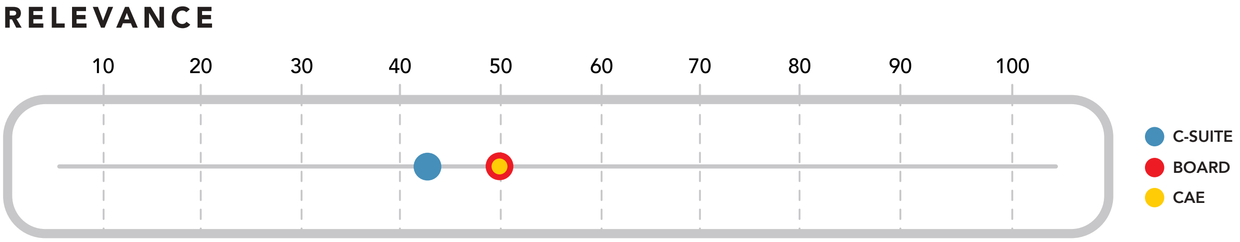
Moved from Develop to Maintain

SUSTAINABILITY



Analysis:

All parties are reasonably well aligned with regard to organizations' capability to manage environmental, social, and governance risks, which collectively comprise sustainability. However, confidence is fairly low. CAEs rate their personal knowledge about this increasingly relevant risk category as very low.



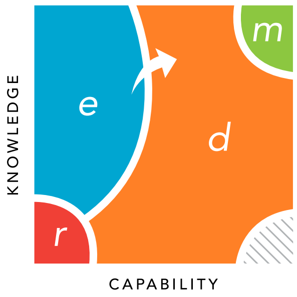
Actions:

C-suite: Recognize sustainability's growing importance to organizational stakeholders, including customers, employees, and investors. Identify opportunities to enhance long-term shareholder value by embracing sustainability leadership as a strategic opportunity.

Board: Pressure management to build sustainability into strategic plans. Set expectations of internal auditors to provide assurance related to voluntary or required sustainability reporting.

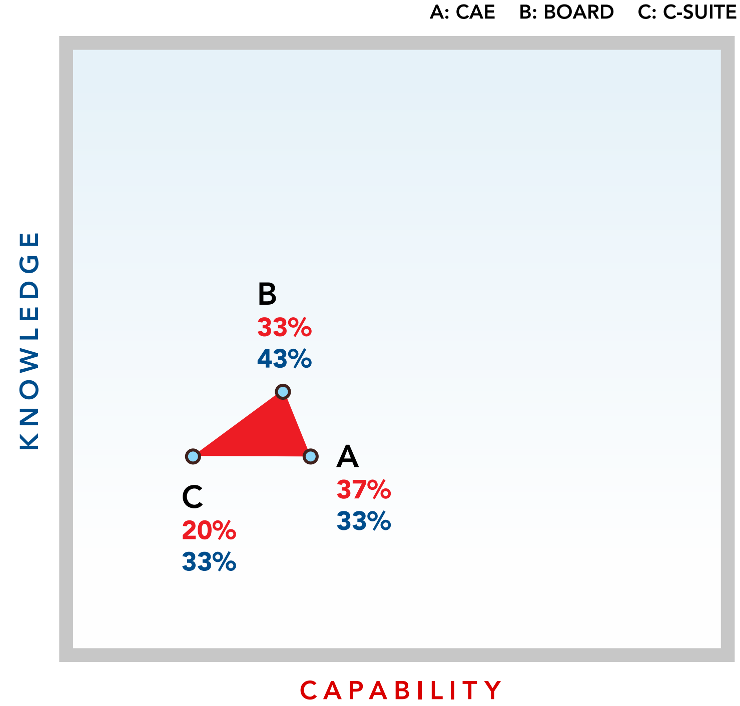
CAE: Educate internal audit teams about emerging risks related to sustainability and how sustainability fits into organizations' operational and strategic priorities.

RISK STAGE



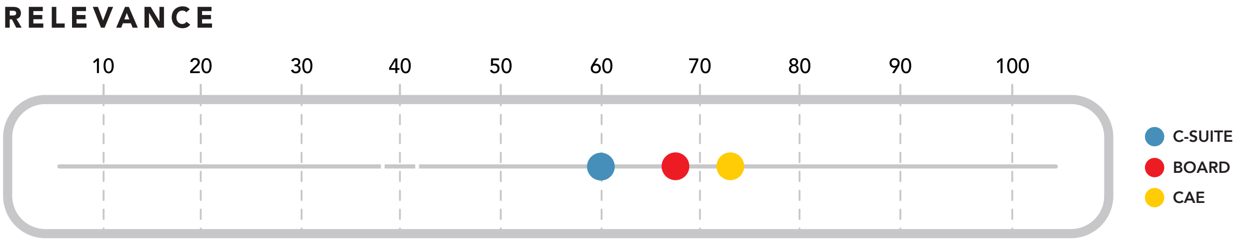
Moved from Explore to Develop

DISRUPTIVE INNOVATION



Analysis:

All risk management roles believe that disruptive innovation is one of the most relevant risks, likely owing to changes in the global economy, exacerbated by the global pandemic. However significant misalignment exists regarding personal knowledge and organizational capability. Boards and CAEs are significantly more confident than management in organizations' capabilities to be appropriately proactive and/or reactive to disruptive innovation. Board members also perceive themselves to be significantly more knowledgeable about risks related to disruptive innovation.



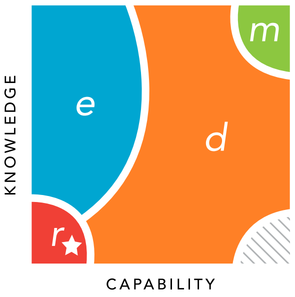
Actions:

C-suite: Leverage the knowledge of board members to identify ways to innovate and identify competitors' attempts to disrupt business as usual.

Board: Share with the organization any guidance and wisdom accumulated through outside and diverse experiences. Set expectations for management to provide proactive strategies that leverage innovation for competitive advantage and to be prepared to react timely to disruption.

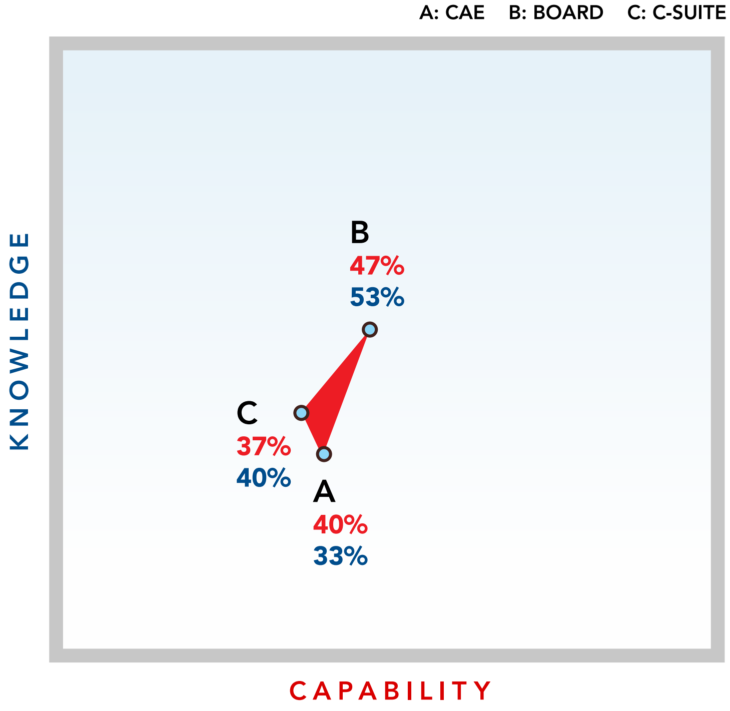
CAE: Ensure a thorough understanding of strategic risks and opportunities to leverage innovation to be disruptive and identify potential risks that could inhibit organizations' strategies to innovate and disrupt.

RISK STAGE



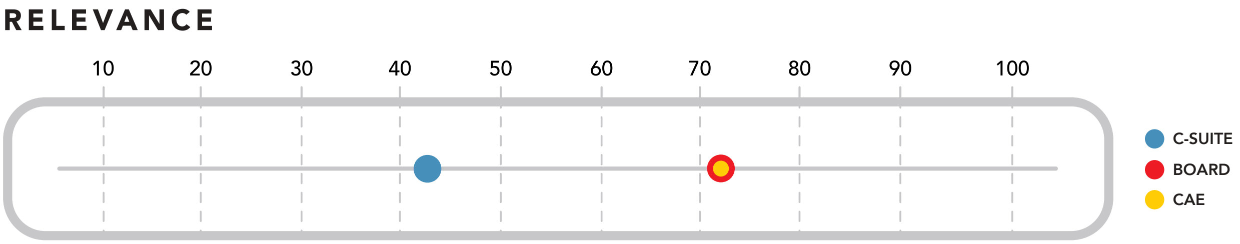
New to OnRisk

ECONOMIC AND POLITICAL VOLATILITY



Analysis:

All parties are aligned regarding the capability of organizations to manage economic and political volatility, but they diverge on levels of personal knowledge about managing external volatility. Further, board members and CAEs are aligned on how relevant this risk is to organizations, but far fewer in management see this as a highly relevant risk.



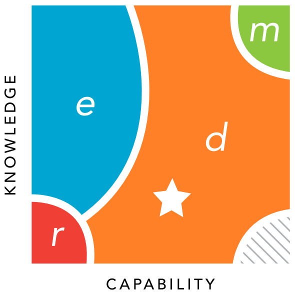
Actions:

C-suite: Build contingencies and scenario plans for dealing with potential outcomes. Communicate with the board about the potential upsides and downsides of political changes and economic swings.

Board: Engage management and internal auditors in discussions regarding potential economic and political outcomes and inquire about the readiness of organizations to be flexible.

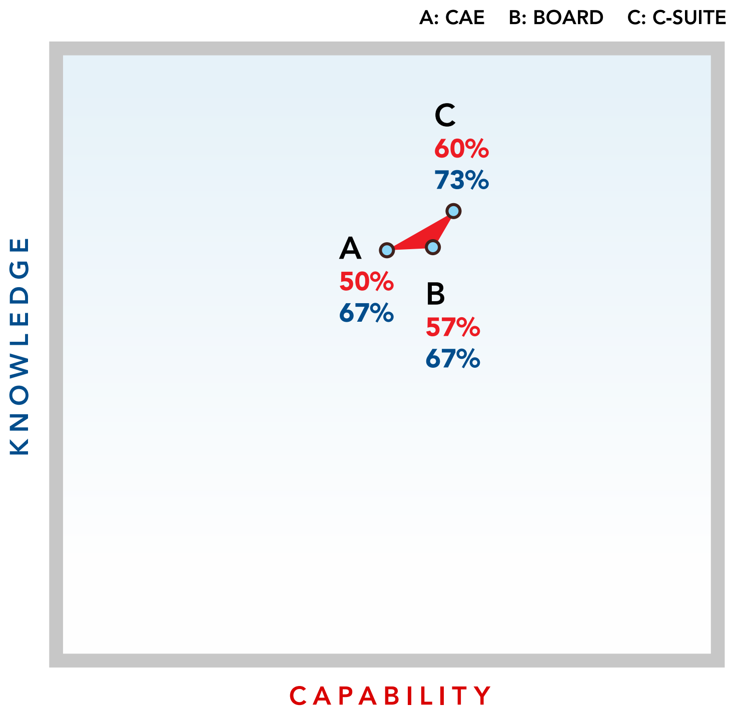
CAE: In order to properly assess organizational capabilities to manage this risk, internal auditors must better educate themselves on how economic and political uncertainties may affect the likelihood of achieving organizational objectives.

RISK STAGE



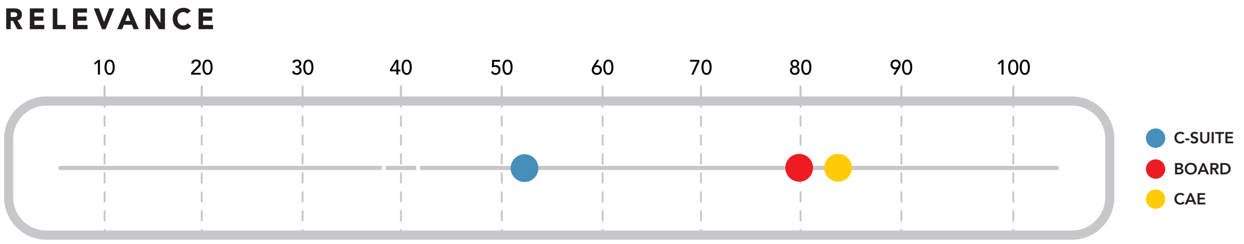
New to OnRisk

ORGANIZATIONAL GOVERNANCE



Analysis:

For this mature risk, there is very strong alignment among all stakeholders regarding individual knowledge and organizational capability. However, while board members and CAEs are well aligned on the relevance of this risk, fewer members of the C-suite see it as highly relevant to organizational ability to achieve objectives.



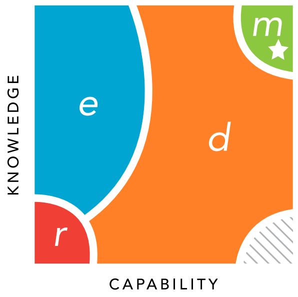
Actions:

C-suite: Align with the board on the relevance of organizational governance and continue to maintain healthy dialogue around risk management and all three key governance roles.

Board: Ensure that senior management understands and agrees upon organizational governance as a priority for achieving organizational objectives.

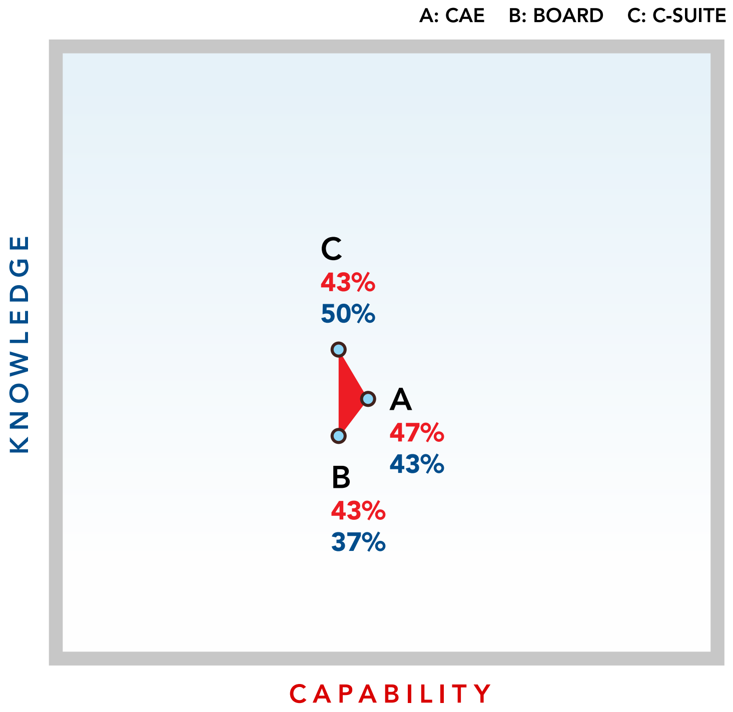
CAE: Maintain a consistent line of communication with board members to ensure their needs are being met.

RISK STAGE



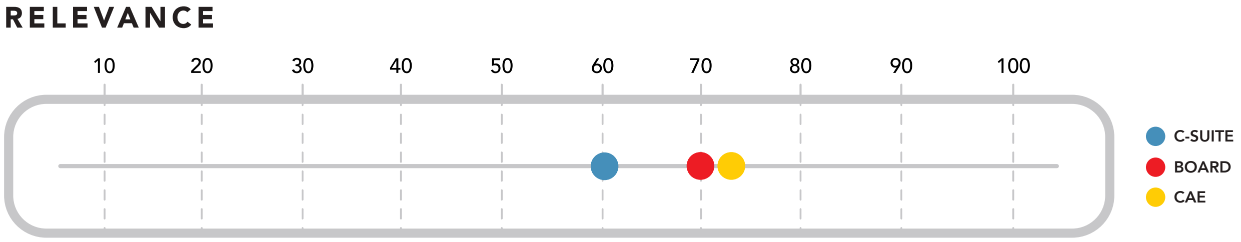
New to OnRisk

DATA GOVERNANCE



Analysis:

There is very strong alignment among all stakeholders regarding organizational capability and reasonable alignment regarding the relevance of this risk to achieving organizational objectives. However, board members view their personal knowledge about the governance over data significantly lower than do either management or CAEs, perhaps because they perceive this governance to be related to the technical aspects of data.



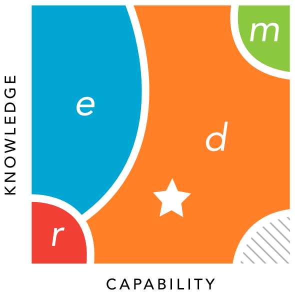
Actions:

C-suite: Drive leading practices in data governance that ensure compliance with laws and regulations as well as progress toward meeting strategic objectives.

Board: Expect education on key aspects of data governance and request briefings from management and internal audit on how the organization strategically manages data.

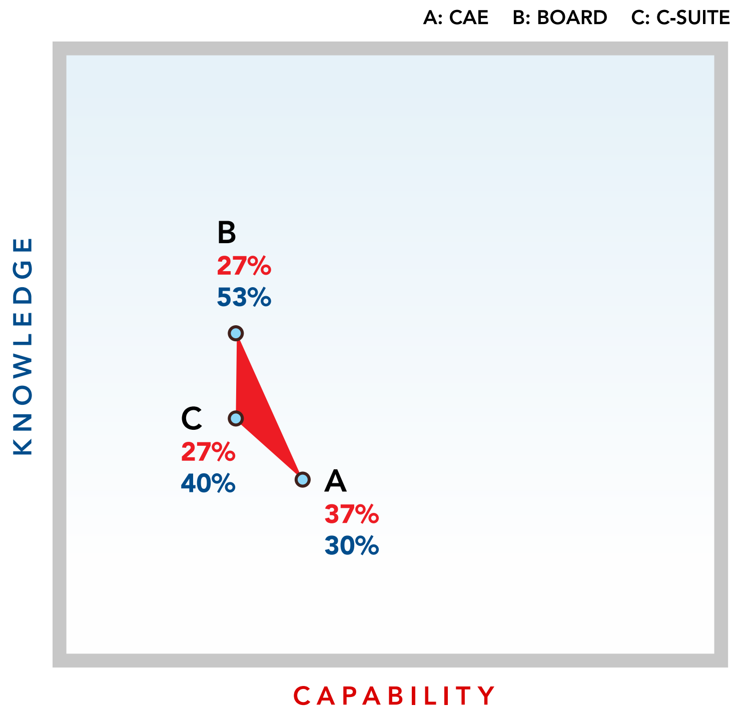
CAE: Provide training to board members on the key aspects of data governance and provide assurance that management practices are leading edge.

RISK STAGE



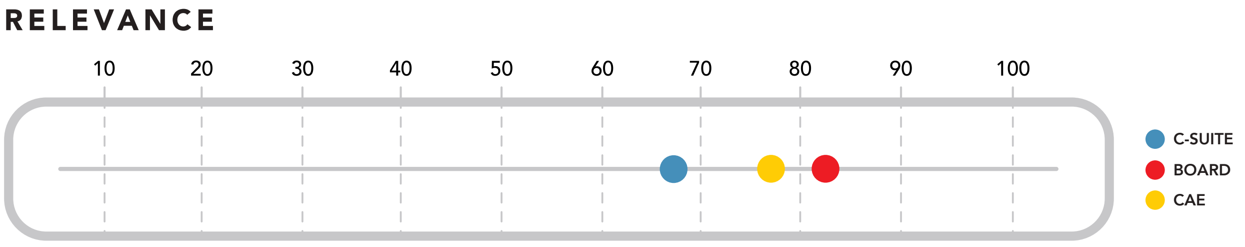
New to OnRisk

TALENT MANAGEMENT



Analysis:

Management and the board agree on organizational capability to address risks related to talent management. However, board members perceive themselves as having greater knowledge and view this risk as having more relevance than do members of management.



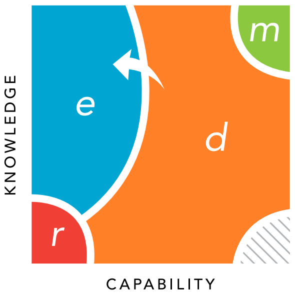
Actions:

C-suite: Focus on evolving the competencies that are most in demand, and develop strategies for ensuring that the organization has and will continue to have the talent to fill those competencies through effective succession planning, upskilling strategies, and recruitment.

Board: Continue to ensure that management is committed to managing talent at all levels of the organization, and set expectations for consistent briefings on talent-related processes and initiatives.

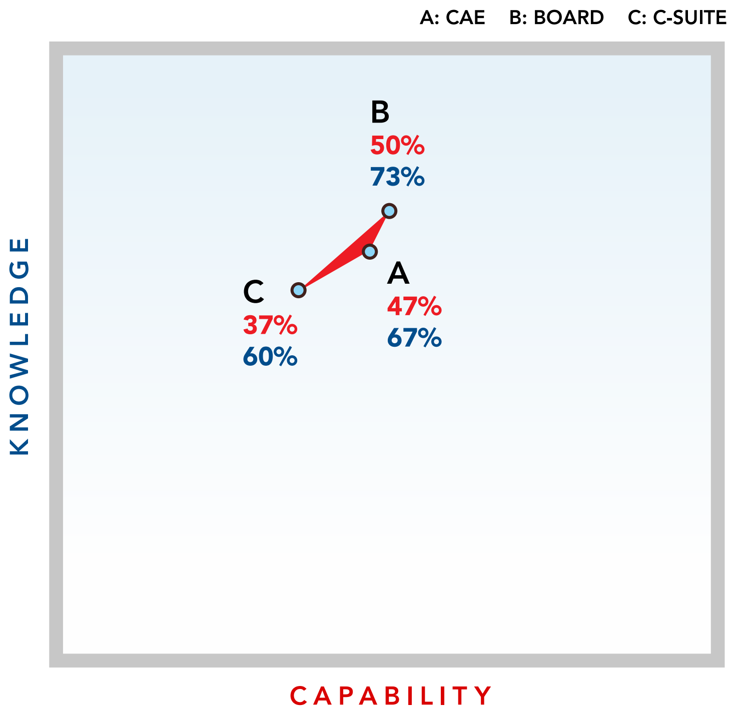
CAE: Consider engagements focused on providing assurance to stakeholders around talent management processes, and maintain open lines of communication with the board regarding its perspectives of key areas of talent focus.

RISK STAGE



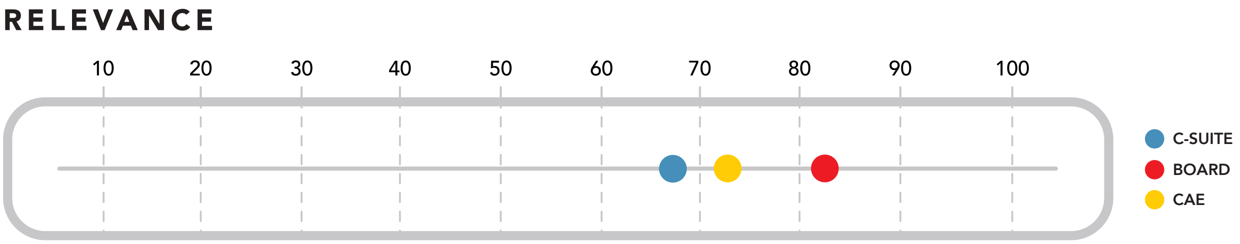
Moved from Develop to Explore

CULTURE



Analysis:

Most of the key players in risk management see culture as highly relevant to organizational success and are relatively confident in their personal knowledge of the topic. However, a significant gap exists with regard to how many feel that their organizations are highly capable of managing this critical risk. Board members, who are inherently more removed from the working culture of the organization, have higher confidence overall than do management respondents and CAEs.



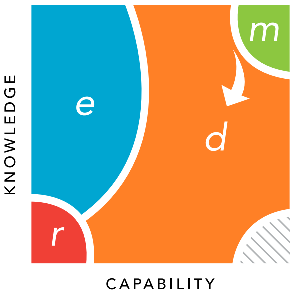
Actions:

C-suite: Act in a manner that promotes an effective culture. Establish consistent processes to gauge the culture and communicate those perceptions to the board timely.

Board: Review assessments of organizational culture with the internal audit function and management. Ensure that executive goals and incentives are aligned with the promotion of an effective organizational culture.

CAE: Consider performing engagements that provide an objective assessment of organizational culture. Provide assurance that management's actions are aligned with leading practices related to organizational culture.

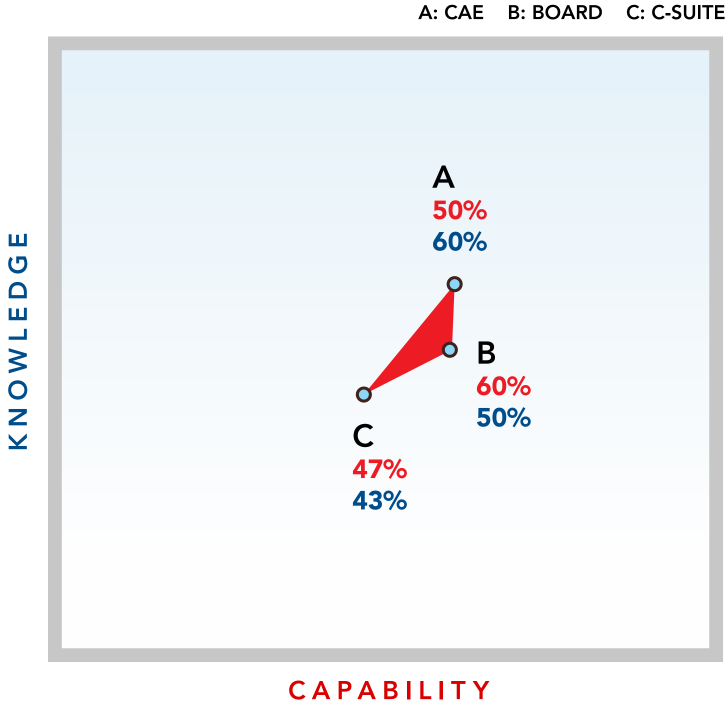
RISK STAGE



Moved from Maintain to Develop

< BACK TO TOC

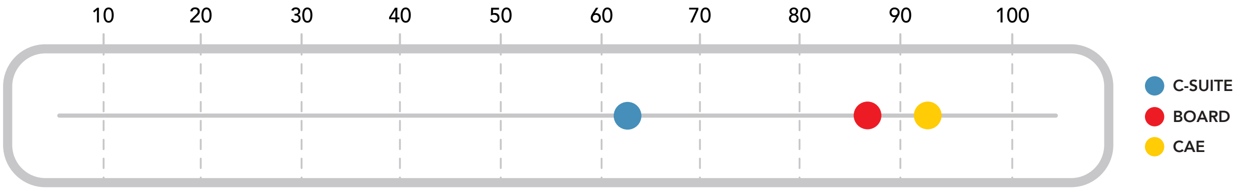
BUSINESS CONTINUITY AND CRISIS MANAGEMENT



Analysis:

Not surprisingly given the events of 2020, nearly all board members and CAEs see this risk as highly relevant to organizations. Ironically, a lower percentage of management respondents see this risk as highly relevant and a significantly lower percentage of management respondents are confident in their organizations' capabilities to manage this key risk.

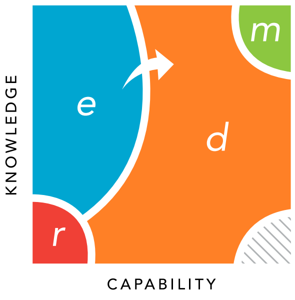
RELEVANCE



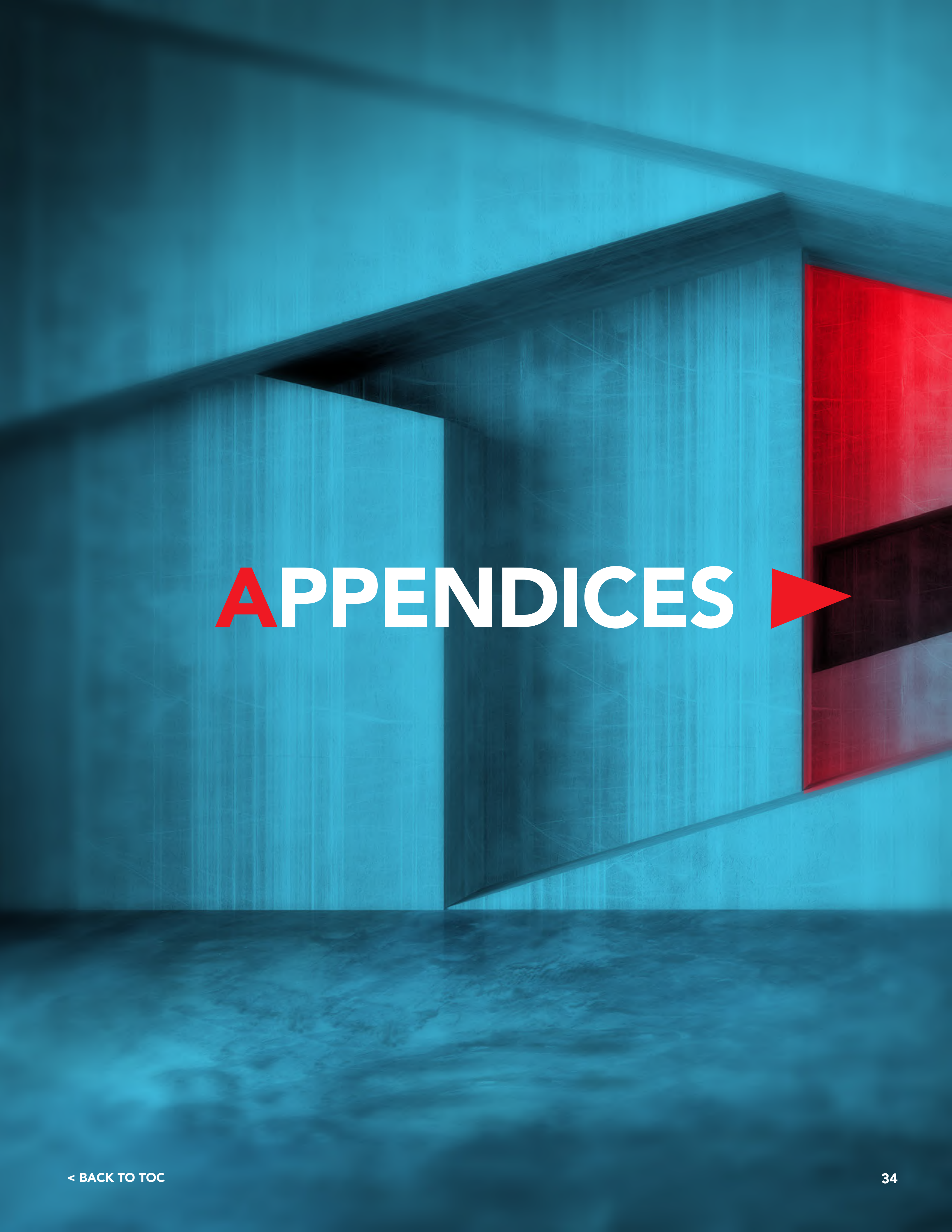
Actions:

All: Leverage experiences of the global pandemic to identify organizational strengths and opportunities for improvement, and work collaboratively to implement improvements where necessary.

RISK STAGE



Moved from Explore to Develop



APPENDICES ►

METHODOLOGY

Qualitative and quantitative surveys

The OnRisk 2021 report continues The IIA's groundbreaking approach of collecting stakeholder perspectives on risk and risk management in support of good governance and achieving organizational success. The combination of quantitative and qualitative research provides a robust look at the top risks facing organizations in 2021. It allows for both objective data analysis and subjective insights based on responses from risk management leaders.

The addition of relevance ratings for each of the 11 key risks provides additional comparative information about how risks are leveraged and managed. While the qualitative and quantitative surveys were limited to organizations based in North America, many of them have global footprints.

The quantitative survey covers top risks as viewed by 348 North American internal audit leaders, primarily CAEs. The comprehensive survey also addressed organizational approaches to risk management, including where internal audit provides assurance and focuses its efforts.

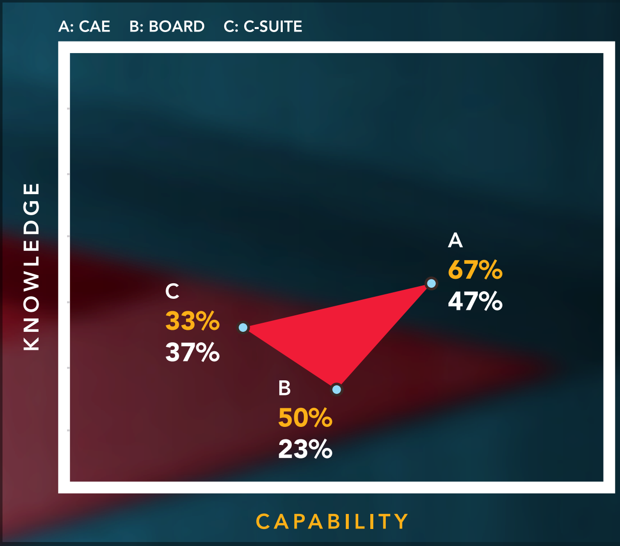


Figure 11: *Personal Knowledge/Organizational Capability Graph*

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

The combined responses for the knowledge and capability ratings 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 11). The plot points were determined by the percentage of respondents who answered a 6 or 7 on the 7-point scale, representing high confidence in personal knowledge and/or organizational capability relating to the risk under consideration. The triangle created by connecting each plot point graphically depicts the alignment among the three respondent groups for each risk.

New this year are the relevance ratings from each respondent group, which are delineated on a single horizontal axis for each risk.

HOW TO USE THIS REPORT

Explanation of graphics

Based on in-depth interviews with 90 professionals, the knowledge and capabilities of each of the three respondent groups were measured and plotted for each risk. Simple quadrant mapping 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 averages for knowledge and capability would be plotted in the top right quadrant. Conversely, responses averaging low for knowledge and capability would be plotted in the lower left quadrant. As described in the previous section, the averages are determined based on the percentage of respondents who provided a top-two rating for the knowledge or capability characteristics.

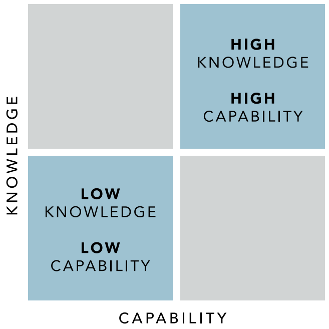


Figure 12: **QUADRANT GRAPH**

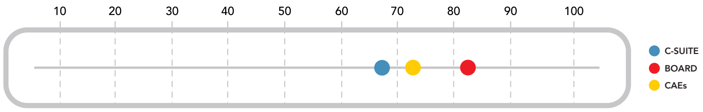
Position plotting

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 any misalignment among the groups that may exist. The resulting triangles — referred to simply as alignment triangles in this report — provide a strong indicator of how well a risk is understood and managed collectively. The size, shape, and location of each triangle also provides insights on what is driving any misalignment (SEE RELATED SIDEBAR).

New relevance graphic

Each respondent group's rating on relevance is plotted along a single axis, providing a clear depiction of variations in the relevance rankings by board members, management, and CAEs.

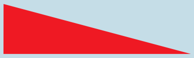
Figure 13: **RELEVANCE GRAPH**



Alignment Triangles:

What do they mean?

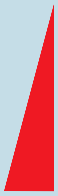
The alignment triangles created by plotting each respondent group's perspectives on each risk offer insights into how the risk is currently being managed. The shape of each triangle can provide valuable information, as well.



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.

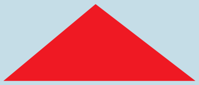
TALL AND NARROW



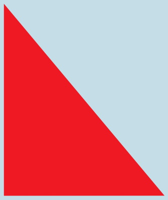
Conversely, triangles with this basic shape suggest significant range of knowledge among respondent groups, but strong alignment on their views on organizational capability.

SHORT AND BROAD

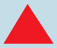
This basic shape suggests disagreement by more than one respondent group, with the most significant disagreement relating to the organization's capability to address the risk.



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 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).

< BACK TO TOC

LEVERAGING THE METHODOLOGY

Readers of OnRisk 2021 should review and analyze the data for each of the 11 key risks addressed in this report and are encouraged to conduct a similar analysis among their own organizations' boards, management, and internal audit functions.

Comments from qualitative interview participants are interspersed throughout OnRisk 2021 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, the organization's capability to manage risk, and the relevance of individual risks to the organization's efforts to set and achieve goals.

A critical step in such an analysis is to undertake a clear-eyed examination of how those charged with risk management understand and execute their roles. The IIA's recently published Three Lines Model provides additional guidance for understanding the essentials of governance and the roles that support those essentials:

- *Accountability — by the governing body (board) to stakeholders for oversight.*
- *Actions (including managing risk) — by management to achieve organizational objectives.*
- *Assurance and advice — by an independent internal audit function to provide insight, confidence, and encouragement for continuous improvement.*

As noted earlier in this report, the COVID-19 pandemic has impelled organizations toward improved communications, ongoing risk assessments, and closer alignment on key risks. When combined with a strong understanding of roles, this new collaboration and communication create ideal conditions for successful risk management and governance.

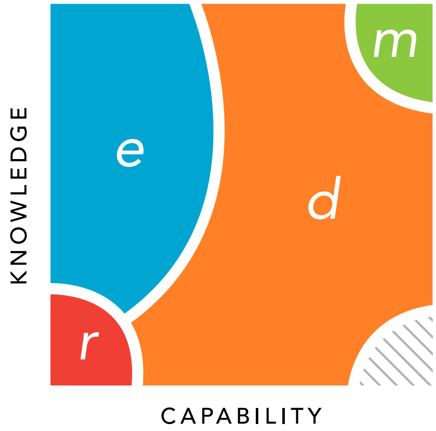
< BACK TO TOC

THE STAGES OF RISK

The risks discussed in this report fall into one of four stages as they relate to the potential impact on organizations and what actions organizations should be taking to address them — recognize, explore, develop, and maintain. The Risk Stages Model (Figure 14) reflects how risk management evolves on the same scale as two of the risk rankings — knowledge and capability.

Additionally, the relevance of each risk should be understood as unique to each organization. Where each risk ranks in relevance depends on various factors including the organization's size, industry, and type as well as competition, maturity, supply chain, liquidity, and other factors. As noted earlier, there are likely risks not included in this analysis that have particular relevance to some organizations, depending on their specific circumstances. Because of this unique aspect, relevance is not depicted in the Risk Stages Model.

Figure 14:
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 stakeholders but not all. The risk may be perceived as emerging or dynamic. Risk response strategies have been contemplated but not 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 have been developed and implemented, consistent with the perceived relevance of the risk. 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

< BACK TO TOC

FIGURES

Figure 1 – OnRisk 2021 Risk Ratings – All Respondents

Source: OnRisk 2021 qualitative survey. Questions: How knowledgeable are you about each of the following risks? How capable is your organization when it comes to handling each of the following risks? How relevant are each of the following risks to your organization? Combined percentage for scores of 6 or 7, with 7 being the highest level. n = 90

Figure 2 – Areas For Improvement: C-suite

Source: OnRisk 2021 qualitative survey: Questions: How capable is your organization when it comes to handling each of the following risks? How relevant are each of the following risks to your organization? Combined percentage for scores of 6 or 7, with 7 being the highest level. n = 30

Figure 3 – Learning Opportunities: C-suite

Source: OnRisk 2021 qualitative survey: How knowledgeable are you about each of the following risks? How relevant are each of the following risks to your organization? Combined percentage for scores of 6 or 7, with 7 being the highest level. n = 30

Figure 4 – Average Rating By Respondent Group

Source: OnRisk 2021 qualitative survey: Questions: How knowledgeable are you about each of the following risks? How capable is your organization when it comes to handling each of the following risks? How relevant are each of the following risks to your organization? Combined percentage for scores of 6 or 7, with 7 being the highest level. n = 90

Figure 5 – Organizational Relevance

Source: OnRisk 2021 qualitative survey: Question: How relevant are each of the following risks to your organization? Combined percentage for scores of 6 or 7, with 7 being the highest level. n = 90

Figure 6 – Organizational Capability

Source: OnRisk 2021 qualitative survey: Question: How capable is your organization 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 = 60

Figure 7 – Organizational Governance

Source: OnRisk 2021 qualitative survey. Questions: How knowledgeable are you about each of the following risks? How capable is your organization when it comes to handling each of the following risks? How relevant are each of the following risks to your organization? Combined percentage for scores of 6 or 7, with 7 being the highest level. n = 60

Figure 8 – The IIA's Three Lines Model

Source: The Institute of Internal Auditors

Figure 9 – Assurance Insights

Source: OnRisk 2021 quantitative survey: Q7. Which of the following risks do you provide or anticipate providing assurance on in 2020 and/or 2021? n = 348. OnRisk 2021 qualitative survey C-suite respondents: How relevant are each of the following risks to your organization? Combined percentage for scores of 6 or 7, with 7 being the highest level. n = 30.

Figure 10 – Tips On Assurance

Source: OnRisk 2021 qualitative survey. Q 11. Where do you get your assurance on the effectiveness of risk management? n = 90

Figure 11 – Personal Knowledge/Organizational Capability Graph

Source: The Institute of Internal Auditors

Figure 12: Quadrant Graph

Source: The Institute of Internal Auditors

Figure 13: Relevance Graph

Source: The Institute of Internal Auditors

Figure 14: Risk Stages Model

Source: The Institute of Internal Auditors

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.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org