

— at the — TONE TOP®

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 107 | October 2021

OnRisk 2022: Timely Insights on Key Risks

The **COVID-19 pandemic** and its many disruptions provided a major wakeup call for organizations on the need to understand the wide variety of risks and uncertainties they face. *OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk*, a report from The Institute of Internal Auditors (IIA), gathered input from the major stakeholders in organizational governance — the board, executive management, and chief audit executives (CAEs) — to determine their alignment on the most relevant risks for organizations right now (see box on page 3) and to gain perspective on the best ways to deal with them. “Boards can use this report to open a dialogue about what issues or concerns apply in their own organizations and what areas may need greater attention,” said Christa Steele, an experienced CEO and public and private company board member.

A review of the report’s key observations reveals not only the major threats for organizations, but also some of the roadblocks that may hinder their ability to address them.

Notable Disparities in Key Areas

OnRisk 2022 offers several key observations, including that significant gaps exist between how relevant respondents believe certain risks are to their organizations and how confident they are in their organization’s ability to address those risks (see chart on page 4). This was determined through analysis of ratings assigned by respondents regarding personal knowledge, organizational capability, and relevance for each risk. The ratings are based on the percentage of respondents who assigned top ratings (a 6 or 7 on a 7-point scale) in each risk area.



Key observations include:

Managing risks requires that organizations have capabilities that are sufficient to the task. Alarming, while cybersecurity was identified as the top relevant risk for organizations by all three respondent groups, *OnRisk 2022* discovered a 45-point gap between those who thought cybersecurity was highly relevant to their organizations (87%) and those who believed their organizations had strong capabilities (42%) in this area. Significant Relevance-Capability gaps were noted for other risk areas, as well. While the pandemic underscored the value of managing qualified people, there was a 46-point Relevance-Capability gap for Talent Management. Several risks that respondents expect to gain relevance in the next three to five years all had large Relevance-Capability gaps, including Culture (36 points), Disruptive Innovation (34 points), and Economic and Political Volatility (32 points).

There were meaningful variations in responses from senior executives, board members, and CAEs on risk relevance and organizational capabilities in a number of risk areas. That’s troubling because when stakeholders’ views on organizational capability and risk relevance are aligned, it is easier to achieve robust risk management.



About The IIA

The Institute of Internal Auditors, Inc. is a global professional association with more than 200,000 members in more than 170 countries and territories. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator.

The IIA

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746 USA

Complimentary Subscriptions

Visit www.theiia.org/Tone to sign up for your complimentary subscription.

Reader Feedback

Send questions/comments to Tone@theiia.org.

When it came to risk relevance, more board members tagged Disruptive Innovation as a highly relevant risk than did senior executives (77% vs. 50%), which was the largest gap in the risk relevance ratings among the three groups surveyed. For Cybersecurity, not only did respondents give their organizations low marks for capability (42%), they were not in full accord on the degree of its relevance. CAEs were more likely to cite it as a highly relevant risk (97%) than board members (87%) or management (77%). CAEs also cited Supplier and Vendor Management risks (77%) as more relevant than did boards (60%) and the C-suite (67%), and were more likely to worry about Economic and Political Volatility (80%) than board members (63%) or senior management (67%).

For ratings on organizational capability, senior executives tended to be more confident in a number of risk areas. One exception was Disruptive Innovation, where only 20% of senior executives rated organizational capability as high – the lowest rating for any capability – compared with 43% of board members. This was the largest split between two groups on capability.

Boards had less confidence than senior executives when it came to the organization's capability to manage risks associated with Talent Management and Environmental Sustainability (a 20-point gap for each) and Organizational Governance (13 points). In each case, boards were more closely aligned with CAEs.

There were differences in perceptions about ESG considerations. The report broke out the three related risk areas: Environmental Sustainability, Social Sustainability, and Organizational Governance. Among them, respondents saw Organizational Governance as having far more relevance than the other two. Given growing interest in this risk area among investors and regulators, boards may want to request an internal audit review of ESG risk management to ensure that all issues are understood and adequately addressed within their organizations.

New Risk Management Opportunities

The pandemic raised awareness about the need to gain assurance in areas beyond financial and compliance risks. External audits focus mainly on these areas, but internal audit can have a broader mandate with board and executive management support. "That includes a wide range of risks, including geopolitical, operations, finance, compliance and legal, and cultural risk," Steele noted. In light of the pandemic, *OnRisk 2022* respondents expressed interest in opportunities for greater assurance on operational and enterprise risk and had a new appreciation for the need to proactively address risks.

QUESTIONS FOR BOARD MEMBERS

- » What risks does our organization face beyond compliance and financial?
- » Has our organization conducted an enterprise risk assessment that addresses new challenges revealed by the COVID-19 pandemic?
- » Does our organization have the capabilities to tackle the risks it faces?
- » Does our board receive the enterprise risk management perspective it needs for good governance?



Steele noted that internal audit has a macro level view of the organization. “They can look down the road and around the corner,” she said. In addition, “At a time when the world is awash in data, they can offer insights on what information should be coming to the board room.” All stakeholders can then work together with the same fact-based data to identify strategies that will focus risk management resources where they are most needed.

Steele recommended that the CAE have a seat at the table with the C-suite so that the audit plan reflects the organization’s strategic initiatives. Expanded use of internal audit services can add value across the board, especially in highly relevant risk areas such as Cybersecurity, Talent Management, and Organizational Governance, which have received greater attention because of the pandemic.

Next Steps for Board Members

The pandemic forced organizations to take a hard look at risk management issues and seek improvements. As the range and intensity of risk impacts grow, internal audit services can be a key partner in ongoing efforts to identify and mitigate threats, offering independent and objective assurance for decision making. As boards consider their next steps, *OnRisk 2022* provides a roadmap to problem areas that may plague many companies and a model that boards can use to consider their own Relevance-Capability gaps.

TOP RISKS OF *ONRISK 2022*

Twelve risks were chosen from a broad list of possible threats that might affect organizations in 2022 and vetted through in-depth interviews with board members, executive management, and CAEs. They are shown here in order of combined risk relevance based on ratings assigned by *OnRisk 2022* respondents, along with a question that sums up related concerns.

Cybersecurity: Are organizations ready to manage cyber threats that could cause disruptions to operations and harm to their reputations?

Talent Management: Given the switch to remote operations and dynamic labor conditions, can organizations face the challenges of identifying, acquiring, training, and retaining the talent they need to achieve their goals?

Organizational Governance: Does governance — its rules, practices, processes, and controls — enhance or hinder achievement of objectives?

Data Privacy: In light of the increasingly complex and dynamic international regulatory environment, does the organization adequately protect sensitive data and ensure compliance with all applicable laws and regulations?

Culture: Given the rise of remote and flexible work arrangements, does the organization understand, monitor, and manage the tone, incentives, and actions that will drive the desired behavior from all employees?

Economic and Political Volatility: Does the organization monitor and address relevant challenges and uncertainties in a dynamic and potentially volatile economic and political environment?

Change in Regulatory Environment: Is the organization, whether heavily regulated or not, prepared to address the risks in a dynamic and ambiguous regulatory environment?

Supplier and Vendor Management: How equipped is the organization to develop and monitor fruitful third-party relationships?

Disruptive Innovation: Can the organization adapt to and/or capitalize on disruption?

Social Sustainability: Is the organization able to understand and manage the direct and indirect impacts its actions have on individuals and communities?

Supply Chain Disruption: Has the organization built in the flexibility necessary to adapt to current and future supply chain disruptions?

Environmental Sustainability: Is the organization able to reliably measure, evaluate, and accurately report on its environmental impacts?

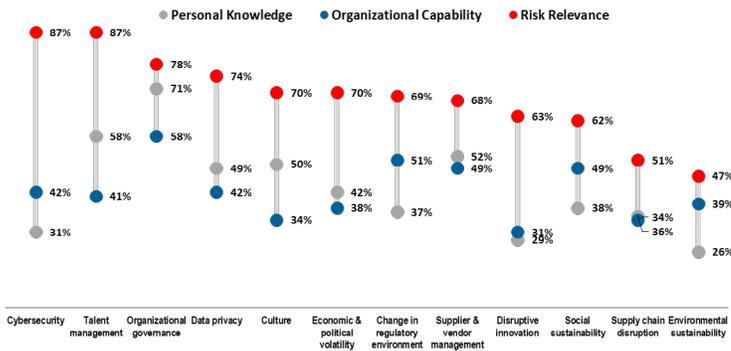


Methodology: The OnRisk Approach

The **OnRisk methodology** employs qualitative interviews of 30 board members, 30 C-suite executives, and 30 CAEs from 90 different organizations. The research provides a robust look at risks facing organizations and allows for both objective data analysis and subjective insights based on responses from risk management leaders. As part of the interviews, respondents were asked to evaluate 12 key risks in three areas: Their personal 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.

Average Ratings Per Risk Area

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



Note: OnRisk 2022 interview questions: How knowledgeable are you about each of the following risks? How relevant are each of the following risks to your current organization? Overall, how capable is your company when it comes to handling enterprisewide risk? Respondents could choose a rating from a scale of 1 to 7, with 1 being the lowest ("not at all") and 7 being the highest ("extremely"). All respondents, n = 90.



Quick Poll Question

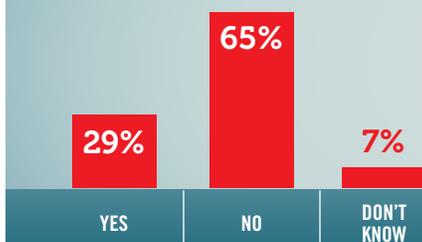
Our board is in alignment with executive management's opinions on the relevance of the risks we face:

- Always
- Often
- Rarely
- Never
- Don't know

Visit www.theiia.org/Tone to answer the question and learn how others are responding.

QUICK POLL RESULTS

Does your board have a member with cybersecurity expertise?



Source: Tone at the Top August 2021 survey.

