TONE at the TOP®

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

Issue 120 | December 2023

Risk Considerations for Directors in 2024

Cybersecurity and human capital were among the top risks identified in a survey aimed at determining current and emerging risks for companies globally and in six different regions. Risk in Focus 2024, published by The Institute of Internal Auditor's (IIA) Internal Audit Foundation, surveyed internal audit leaders on the current risk environment for their organizations (see Figure 1) and on which areas they are focusing on in their audit plans . It also asked them to project which risks will be most significant in the next three years.

This issue of Tone at the Top addresses some of the top risks they identified. As boards consider new and emerging threats, internal audit can be an important partner in their governance efforts. "Internal auditors are taking a proactive approach to risk," said Javier Faleato, CIA, CRMA, CCSA, The IIA's executive vice president, global relations. "They are walking with companies on their journeys and helping them take the right road."

Putting Cybersecurity Risk into Perspective

As cyber criminals have grown more sophisticated in recent years, many boards have added cybersecurity expertise, but it can be challenging to determine how efforts discussed in technology jargon can apply to business operations. Internal audit is uniquely positioned to serve as a translator, making the connection between cyberthreats and potential business risks, Faleato said. Internal audit leaders can update boards on new cybersecurity developments and incidents that are impacting the organization and on how they affect risk management and strategic planning. Internal audit can also review the effectiveness of governance processes around cybersecurity. "Internal audit's role is to make boards aware of what's working and what's not," he said.

Top % highest risks per region

What are the top 5 risks your organization currently faces?

Audit area	Average of all regions	Asia Pacific	Latin America	Africa	North America	Middle East	Europe
Cybersecurity	73%	66%	75%	58%	85%	70%	84%
Human capital	51%	59%	44%	39%	65%	47%	50%
Business continuity	47%	61%	47%	52%	36%	53%	35%
Regulatory change	39%	35%	48%	32%	43%	33%	43%
Digital disruption	34%	30%	38%	33%	36%	32%	33%
Financial Liquidity	32%	21%	33%	47%	28%	38%	26%
Market changes	32%	47%	26%	21%	41%	26%	30%
Geopolitical uncertainty	30%	28%	42%	25%	28%	16%	43%
Governance/corporate reporting	27%	24%	18%	36%	16%	45%	22%
Supply chain and outsourcing	26%	27%	16%	19%	36%	28%	30%
Organization culture	26%	23%	26%	34%	21%	30%	20%
Fraud	24%	22%	30%	46%	9%	26%	13%
Communications/reputation	21%	18%	22%	27%	21%	28%	12%
Climate change	19%	22%	22%	19%	12%	10%	31%
Health and safety	11%	12%	8%	10%	17%	9%	13%
Mergers and acquisitions	6%	4%	3%	3%	8%	10%	8%

Figure 1

Source: Risk in Focus 2024

Note: The IIA's Risk in Focus Global Survey, n=4,207. Percentages show who ranked the area as one of their top 5 for risk level. Dark blue shading indicates the 5 areas of highest risk for that region.

The internal audit team can also provide insights on whether the company is doing all that is necessary to mitigate related threats. Overall, the survey found that internal audit teams are putting a higher emphasis on cybersecurity in their audit planning. Although cybersecurity has long topped the list of Risk in Focus concerns, in the past audit teams were not placing the most time and effort into this area. That has changed, according to this year's survey, with cybersecurity generally well ahead of other focuses for audit teams. Boards can safeguard that internal audit teams continue to maintain an appropriate focus by ensuring that they have sufficient resources to address cybersecurity issues.

It's an unfortunate fact that the greatest cybersecurity vulnerability in most organizations is the human element. Employees are targeted by phishing emails or other increasingly sophisticated schemes designed to give cybercriminals access. Directors should remember the importance of tone at the top when it comes to cybersecurity, and the positive impact that boards can have. When employees see that board members are aware of and involved in cybersecurity efforts, they may be less likely to neglect smart cyber safety protocols, Faleato said. Boards might consider taking part in corporate training on phishing attack campaigns, for example, and engaging in board-level, ransom attack scenarios with support from internal audit, he recommended.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 230,000 global members and has awarded more than 185,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Complimentary Subscriptions

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

Reader Feedback

Send questions/comments to Tone@theiia.org.

Governance for the Most Important Corporate Asset

Employees' talent and expertise are critical to company success. Organizations understand that human capital, diversity, equity and inclusion, and talent management and retention are key concerns, but many do not know or are uncertain how to measure whether efforts in these areas are having a meaningful impact. The conversation has become even more complicated because of the changing expectations of new generations of employees and the ongoing debate over remote and hybrid work schedules.

Given the stakes and uncertainties, boards need clear information and advice. Internal audit can help boards determine which human capital metrics are most valuable to the board and present complex key performance indicators (KPIs) in ways that are easy to understand from a strategic and governance perspective. For example, internal audit has access to a wide range of insightful corporate information, including employee satisfaction measures that the board can use to better align human capital and diversity strategies with changing cultural norms and expectations.

Preparing for Emerging Risks

Risk in Focus 2024 asked internal audit leaders to rank which risks their organizations would be facing three years from now (see Figure 2). Not surprisingly, cybersecurity remained the top choice. However, digital disruption moved from the fifth spot today to second, and climate change jumped from fourteenth to fifth. Here's what directors should be considering in each area.

Expected risk change in 3 years

What are the top 5 risks your organization currently faces?		What are the top 5 risks your organization currently faces?	
1. Cybersecurity	73%	1. Cybersecurity	67%
2. Human capital	51%	2. Digital disruption	55%
3. Business continuity	47%	3. Human capital	46%
4. Regulatory change	39%	4. Business continuity	41%
5. Digital disruption	34%	5. Climate change	39%
6. Financial Liquidity	32%	6. Regulatory change	39%
7. Market changes	32%	7. Geopolitical uncertainty	34%
8. Geopolitical uncertainty	30%	8. Market changes	33%
9. Governance/corporate reporting	27%	9. Supply chain and outsourcing	25%
10. Supply chain and outsourcing	26%	10. Financial Liquidity	23%
11. Organization culture	26%	11. Organization culture	21%
12. Fraud	24%	12. Governance/corporate reporting	20%
13. Communications/reputation	21%	13. Fraud	20%
14. Climate change	19%	14. Communications/reputation	15%
15. Health and safety	11%	15. Health and safety	11%
16. Mergers and acquisitions	6%	16. Mergers and acquisitions	11%

Figure 2

Source: Risk in Focus 2024
The IIA's Risk in Focus Global Survey, n=4,207. Percentage who ranked the area as one of their organization's top 5 highest risks.

Digital disruption. It's difficult to know which new technologies will have the most impact over the near term, but it's likely that generative artificial intelligence (AI) will be one of them. The first well-known example of generative AI, ChatGPT, reached an estimated 100 million users within a couple of months of its launch [i]. AI overall, and generative AI in particular, are set to change the way businesses are run. Internal audit can help boards understand the huge opportunities they can offer, as well as the significant risks, Faleato said. After generative AI's initial enthusiastic public reception, many questions have arisen about related ethical and legal concerns. They include risks involving privacy and confidentiality, lack of transparency of source material, intellectual property considerations, and information accuracy. As the technology evolves and use grows, internal audit can alert the board to the risks and benefits and provide advice on managing them.

Climate change. Corporate reporting in this area has long been voluntary, but that is changing rapidly as regulators issue or propose new regulations. These include the European Sustainability Reporting Standards, a proposal on climate-change related disclosures from the U.S. Securities and Exchange Commission, and new guidance from the International Sustainability Standards Board, as well as national regulations in Australia, Canada, India, Brazil, Singapore and others. Internal audit can update boards with some of the new concepts involved in this area. For example, while organizations have long understood the concept of materiality when it comes to financial risk, they will now have to become familiar with the concept of double materiality.

This concept describes how corporate disclosures can be important both for their implications about an organization's financial value, and about an organization's impact on the world at large. "The idea of double materiality comes from a recognition that a company's impact on the world beyond finance can be material, and therefore worth disclosing, for reasons other than the effect on a firm's bottom line[ii]."

"The board will need people they can trust to provide assurance on the assumptions behind decisions on double materiality reporting," Faleato said. Internal auditors, who have a deep familiarity with the organization, its business, and processes, can offer thorough and reliable assurance.

"Greenwashing" is another concept that boards should be familiar with. It refers to making inflated or false claims about an organization's climate change policies or actions. Being accused of greenwashing can have a significant impact on an organization's reputation, particularly given the large and varied group of stakeholders calling for more transparency in environmental reporting. Internal audit can enhance confidence in the climate-related information that organizations report by providing assurance on it. Internal audit can bring all these topics to the board table and provide the context directors need to address them.

The Interconnectivity of Risks

Risk in Focus 2024 also highlighted the interconnectivity of risks—the way in which one risk can cause and even magnify others, Faleato noted. For example, a cybersecurity incident is usually not merely a headache for the IT team or for any employees directly affected by it. Among other negative impacts, it can frequently have a negative impact on the organization's brand or supply chain relationships, if customers, business partners, or other stakeholders are involved. "You can't look at risks as isolated incidents," Faleato said.

Internal audit can offer boards a perspective that connects the dots and makes sense of the wide range of seemingly unrelated risks they face. Faleato recommended that boards or audit committees meet regularly with internal audit leaders to discuss risk management, compliance concerns, business opportunities, and process efficiencies. "We can be a business partner in all these areas," Faleato said. "That's our great value for boards."

QUESTIONS FOR BOARD MEMBERS

- How is the board preparing for regulations on disclosing environmental, social and governance information?
- What regulations have or are expected to have an impact on the organization?
- Will we be expected to provide ESG information to business partners or other members of our value chain?
- Can the organization generate reliable ESG information for use in strategic decision making

i"ChatGPT sets record for fastest-growing user base - analyst note," Hu, K., Reuters, Feb. 2, 2023
ii"Double materiality': New legal concept likely to play in debate over SEC's climate plan," ," Engler, H., Reuters, April 12, 2022.