

— TONE — at the — TOP[®]

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

Issue 110 | April 2022

Risk Considerations for Boards

As boards consider how to operate in a riskier world, it's important to examine priorities for how internal audit and audit plans are being used. The IIA's [2022 North American Pulse of Internal Audit](#) report confirms that an array of risks remain top of mind for chief audit executives (CAEs). At the same time, a majority of boards of directors have raised or expect to raise their risk appetite this year, according to a [Gartner survey](#). That's not surprising, given the uncertainty of the last two years and the ongoing unexpected developments affecting domestic and global economies.

Yet, these risks aren't necessarily being reflected in audit plans.

This issue looks at risks in two key areas — cybersecurity and sustainability issues — and examines how organizations and boards are reflecting their concerns to internal audit for inclusion in audit plans. We'll also consider the value that internal audit can offer boards, and how boards can ensure they make the most of that value.

Cyber Risks Rising

In the [Pulse survey](#), the top three highest risk areas cited by CAEs were all technology related: cybersecurity, IT, and third-party relationships (which often include IT services). One of these three stood out: cybersecurity. Pulse data show that 85% of CAEs rate cybersecurity as a high or very high risk in their organizations.

This emphasis on cybersecurity risk from internal audit is in line with the expectations boards are facing. According to PwC's Governance Insights Center, "Stakeholders demand that companies do everything in their power to protect consumer data, and to also recover quickly from a breach or critical disruption." It notes in its publication, [Overseeing Cyber Risk: The Board's Role](#), that data security and privacy fall under "an area of heavy focus from multiple stakeholders these days." With that in mind, directors must "maintain an adequate level of cyber knowledge to understand the nature of current risks and provide strategic direction in protecting the organization against them."



Reporting cyber risk considerations is an area of mounting focus. The Securities and Exchange Commission (SEC) in March proposed amendments to its rules to enhance and standardize disclosures by public companies on [cybersecurity risk management, strategy, governance, and incident disclosure](#). Among other things, the proposal would require current reporting about material cybersecurity incidents as well as periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks, detail management's role in implementing them, and evaluate the board's cybersecurity expertise and oversight of cybersecurity risk.

Faced with ongoing cyber threats and rising expectations about governance in this area, boards must be sure to gain the greatest value from the resources available to them, including internal audit. "Boards should ... be hearing from groups such as internal audit about cyber risks," said PwC in its report. "Many companies leverage internal audit to review cyber processes and controls, including resilience and response."

About The IIA

The Institute of Internal Auditors, Inc. is a global professional association with more than 210,000 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 401
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.

The Importance of Sustainability

For the first time in Pulse survey history, sustainability and nonfinancial reporting risk levels edged upward, especially for publicly traded organizations.

In the survey, 40% of CAEs identified one of two areas that fall under the environmental, social, and governance (ESG) rubric as being at high or very high risk levels: governance and culture (28%), and sustainability/nonfinancial reporting (12%). At the same time, the need for assurance over sustainability is ramping up quickly. The SEC has [proposed new climate-related disclosure rules](#) to give investors more consistent, comparable, decision-useful information and provide more uniform and clear rules for issuers. At the same time, the new [International Sustainability Standards Board](#) aims to add greater consistency and reliability to ESG reporting and has issued draft climate-related and general reporting standards currently out for comment. These developments point to numerous new risks that must be considered, as well as new compliance considerations, controls, and processes that require validation by internal audit.

Adjusting Audit Plan Priorities

Boards clearly also agree on the importance of these issues. When asked to identify top strategic business priorities for 2022 and 2023, 32% of directors cited ESG, health, and sustainability, Gartner said. This was the third highest percentage of the priorities listed, and it was up 100% from the previous year.

However, the boost in concern has not yet been seen in audit plans, according to the Pulse survey. The results show that although CAEs have identified both cybersecurity and ESG as risks, boards may not be offering sufficient support to ensure that these risks are adequately represented in audit plans. Indeed, the survey found that while 85% of CAEs rate cybersecurity as a high or very risk in their organizations, cybersecurity audits account for only 11% of the average audit plan. Similarly, a growing number of CAEs identified sustainability as a high or very high risk (12% in 2021, up from 4% in 2020), yet sustainability audits account for just 1% of the average audit plan.

Audit plans should appropriately reflect the board's concerns, and cybersecurity and ESG are certainly on the list. Boards should advocate for cybersecurity, sustainability, and other top risks to be included at a sufficient level in audit plans. When the internal audit function is able to gather the insights and information it needs in these areas, it ensures that the board and management receive a thorough, objective understanding of the threats facing the organization. One critical mistake here would be for boards to assume that external audit is providing all the assurance the organization needs regarding cybersecurity and sustainability/nonfinancial reporting. Internal audit's inside perspective provides deeper and broader insight, reflected in its objective, independent assurance on risks and controls before review by external audit.

The next section will highlight the strategic benefits of enhanced investments in internal audit resources.

QUESTIONS FOR BOARD MEMBERS

- » What is internal audit's current involvement in our ESG assessment and strategy? In cybersecurity assessment?
- » Does our board understand the benefits that internal audit can offer in ESG and cybersecurity strategy assessment and development?
- » Is our investment in internal audit sufficient to provide the resources it needs to offer perspective in top risk areas, such as ESG and cybersecurity?

Boards disclosing oversight of ESG/sustainability

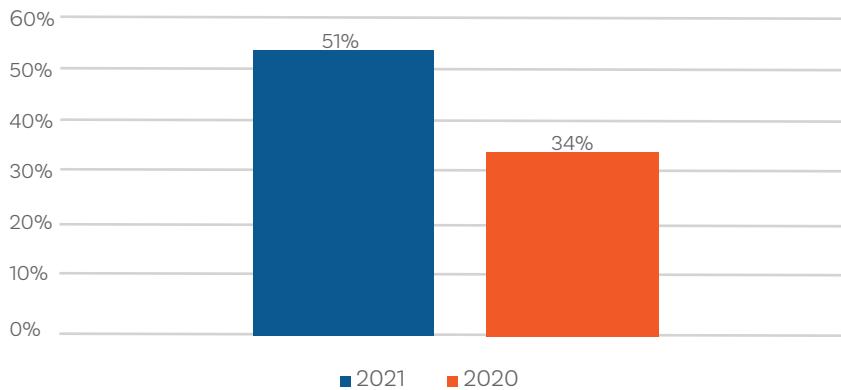


Figure 1 - Source: *2021 Inside the Public Company Boardroom*, National Association of Corporate Directors.

The Importance of Smart Investments

Boards will get the best benefits from the advice and insights that internal audit can offer when the internal audit function has the people and resources it needs. When the Pulse survey asked which types of support would help their internal audit functions most with increasing or maintaining maturity, CAEs' first choices were technology tools (56%) and the ability to hire more skilled or competent staff (52%). Underscoring the point, when CAEs were asked how they would spend additional budget funds, almost half (48%) said their top priority would be to increase staff, while 25% chose to improve technology. Other issues revealed include:

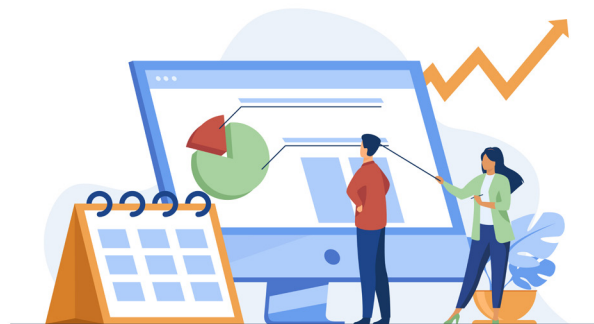
- **Staffing.** The “Great Resignation,” or an increase in voluntary turnover since the height of pandemic, appears to have hit internal audit. While some internal audit staff numbers were normalizing after cuts during the pandemic, budget and staffing levels are not being increased, the Pulse survey found. This may be a result of lower confidence and greater uncertainty about the future, or it could be a result of the difficulty in finding talent. In either case, an adequate team of highly skilled internal auditors can provide the best value for an organization’s investment.

- **Technology.** In the Pulse survey, when CAEs were asked how they would use additional funds in their technology budgets, 68% said that they would spend them on data analytics software. Other picks included robotic process automation software (34%) and artificial intelligence (31%). This is in line with recent findings from the World Economic Forum (WEF); a broad range of digital and related “fourth industrial revolution” technologies “emerged as a key driver of resilient supply chains, helping companies survive the pandemic,” according to its report, *How Fourth Industrial Revolution Tech Helped Companies Survive the COVID Crisis*. “Companies that invest in these technologies can save money and increase their agility in dealing with future challenges,” WEF said. Boards should be aware that advanced digital resources can enable internal audit to provide real-time, thorough analysis and enhance its agility.

Pulse survey respondents whose teams have seen reductions in the past 12 months said that both budgets and staffing had returned to near pre-COVID-19 levels. However, only a small number reported budget increases over pre-pandemic levels. Some even saw lower percentage growth in 2021 than 2020.

Leveraging the Internal Audit Function

Internal audit has navigated the pandemic well. However, given the challenges facing internal audit teams and their organizations, boards should be alert to constraints on internal audit budgets, audit plan priorities, and staffing. In the end, it is the board's responsibility to make the best use of the internal audit function and the independent assurance and insights it provides. Internal audit is a powerful tool for the board and one that can help directors protect their organizations from a wide array of current and emerging risks.



Quick Poll Question

Is the board aware of whether the internal audit plan reflects the organization's risk priorities?

- Yes
- No

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



Copyright © 2022 by The Institute of Internal Auditors, Inc. All rights reserved.