TONE at the TOP®

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

Issue 116 | April 2023

Adjusting the Risk Appetite for Non-Financial Measures

Risk appetite — the level of risk that an organization is prepared to accept in pursuit of its objectives — is fundamental to effective governance in all organizations, and boards play a critical role in setting that appetite. But are credit and market risks and other financial factors the only issues that should be considered? Despite their name, non-financial risks can also have a significant financial impact on an organization. As companies focus on governance, risk, and compliance concerns, they should consider how non-financial risk is impacting the success of their enterprise risk management (ERM) efforts and overall risk appetite.

The sheer number of risks that fall into the non-financial category raises the chances that some may be overlooked. They may include operational, compliance, cybersecurity, reputational, environmental, employee conduct, ethical and corporate culture, public health, social justice, diversity, equity and inclusion, human rights, strategic, third-party, geopolitical, natural resources, human resources, and data integrity risk—among others. This partial list shows just how significant non-financial risks can be and makes the case for incorporating them into any discussion on risk appetite. Indeed, "non-financial risks now pose a potentially costlier threat than financial exposures," according to PwC.[1]

"Non-financial risks now pose a potentially costlier threat than financial exposures." PwC

Expecting the Unexpected

Organizations should be aware that this is an evolving area where new and unfamiliar risks should be expected to emerge. Five years ago, for example, few companies had protocols in place to deal with a potential global health crisis that would interrupt worldwide economic activity, upend supply chains, and bring some industries to a virtual halt, but the COVID-19 pandemic highlighted the need to expect the unexpected.

Even when organizations believe they have their arms around potential non-financial risks, they may not anticipate all the issues that can arise. Privacy risk, for example, seems like a well-known consideration, but it can become a problem in unexpected ways. One well-known retailer experienced reputational damage when it was reported that a parking system app used by its landlord was tracking customers' browser usage. In the uproar that ensued, the retailer argued that it was not in charge of the app, but the reputational damage was done.

The board has an important role in this effort. Regarding environmental, social and governance (ESG) issues, which encompass many common types of non-financial risk, "boards need to continuously examine and question information provided by management and recognize that ESG is an enterprise-level risk that should be viewed through the lens of strategy and operations," according to a National Association of Corporate Directors report.[2]

An Alphabet Soup

Identifying and measuring non-financial risk is an important concern, but there is little consistency in guidance on how this should be done. There is currently an alphabet soup of frameworks and standards that organizations can choose to use but no actual comprehensive requirements at the federal level in the United States and no globally embraced standards. For the moment, the available guidance covers a number of different areas, as demonstrated by the 23 non-financial measurement and reporting standards and frameworks in a list compiled by the Center for Sustainable Organizations.[3] They are categorized based on considerations such as primary constituency of interest (shareholder versus stakeholder), performance constructs of interest (risk, value creation/impact valuation, sustainability), triple bottom line considerations, and primary form of measurement (incrementalist versus context based). Organizations can choose to follow one set of guidelines, to mix and match rules from more than one, or to opt out of this type of reporting altogether. However, the latter may not be a truly viable option going forward. Internal audit can provide insights to help organizations make sense of measurement and reporting options at a time when there is increasing pressure on organizations from a wide range of stakeholders who want more information and transparency on non-financial issues, including ESG. For some of the world's largest institutional investors, "ESG has become a proxy for good risk management and long-termism, two primary concerns today," according to management consulting firm Russell Reynolds Associates. [4]

ISSB REPORTING STANDARDS

In November 2021, the IFRS Foundation trustees announced the creation of a new standard-setting board—the International Sustainability Standards Board (ISSB)—to help meet demands for high-quality, transparent, reliable, and comparable reporting by companies on climate and other environmental, social and governance (ESG) matters.

The ISSB was tasked with developing a comprehensive global baseline of sustainability-related disclosure standards that provide investors and other capital market participants with information about companies' sustainability-related risks and opportunities to help them make informed decisions.

The new ISSB reporting standards addressing climate and sustainability reporting are expected to be published by the end of the second quarter of 2023.

An Evolving Regulatory Landscape

The number of disclosure regulations involving non-financial risk is growing rapidly worldwide, with European Union regulators leading the way. In the U.S., reporting regulations in two non-financial areas are on the imminent horizon. Last year, the U.S. Securities and Exchange Commission (SEC) proposed to require registrants to include specified climate-related and cybersecurity disclosures in their registration statements and periodic reports. For climate concerns, disclosures would include details on risks that could have a material impact on the business, results of operations, or financial condition, along with some climate-related financial statement metrics and disclosures on greenhouse gas emissions. [5] Regarding cybersecurity, there would be amendments to the commission's rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. [6] Although the proposals are aimed at listed companies, private company stakeholders may also press for similar disclosures.

Gathering Non-Financial Risk Data

Many organizations may have some well-established procedures in place related to specific non-financial information, so it's important to understand what data is already available, especially if reporting and disclosure becomes mandatory in some areas. Companies likely have collected a great deal of data for compliance with rules set by regulatory bodies. In the U.S., examples include the Environmental Protection Agency, Occupational Safety and Health Administration, Department of Labor, Department of Commerce, and others. Risk management procedures related to COSO's internal control framework and ISO management systems may also be capturing information on non-financial issues. Internal audit can help companies assess the data on hand to identify information gaps and to avoid duplication of efforts.

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

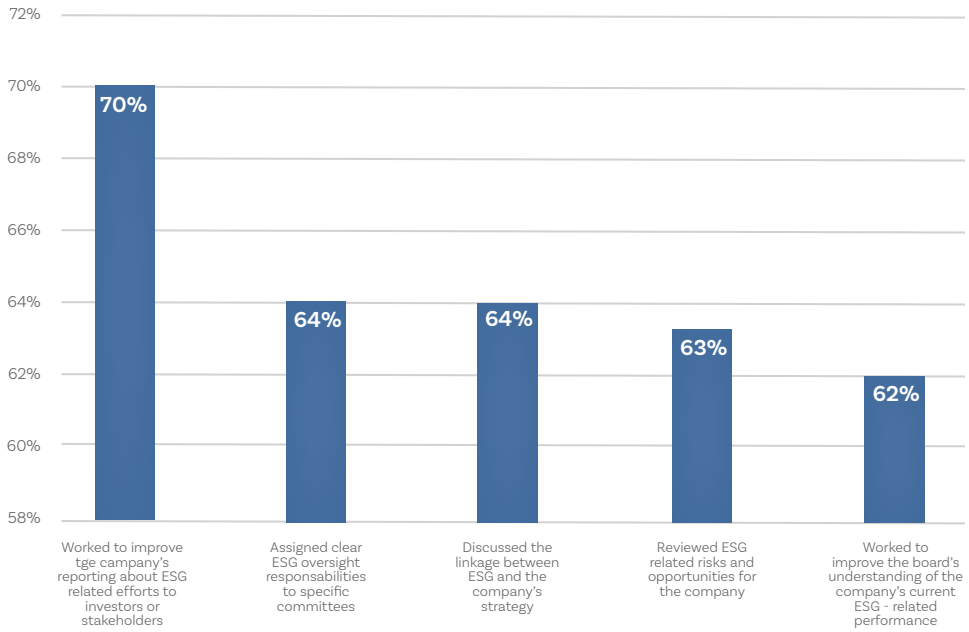
Complimentary Subscriptions

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

However, even though companies may already have information, it's important to be aware that, because of the lack of consistent reporting requirements for non-financial risks and lack of familiarity with this area, the processes and procedures around them may be inadequate. Controls and risk assessment procedures may be less developed in some functions than in others, or insufficient for current needs. The information may be coming from a range of areas—such as human resources, procurement, ESG, or sales—making it challenging to identify and gather. Regarding ESG, "fraud risk in this area should be top of mind for audit committees and a focal point in fraud risk assessments overseen by the audit committee," according to a Deloitte report, which noted that this risk is not governed by the same types of controls present in financial reporting processes. As a result, it may be easier to manipulate voluntarily reported data on carbon emissions or other key non-financial measures. [7]

Private companies may find their controls are lacking. There's clearly room for boards to make a difference on this front. Fourteen percent of private companies told the NACD that their boards had not focused on ESG issues over the past 12 months, compared to only 3% at public companies, which face more demands for data in this area. Only 39% of private companies said their board has reviewed ESG-related risks and opportunities for the company. [8] (See figure 1.)

Figure 1 - **Which ESG Oversight Practices Have Boards Performed in the Last 12 Months?**



Source: : 2022 NACD Board Practices and Oversight Survey—ESG: Compare and Contrast Among Public and Private Companies

Involving Internal Audit

To help leadership understand and tackle non-financial risks, internal audit leaders can use their holistic understanding of the entity's many facets—and threats-to identify risk considerations and provide advice on how best to deal with them.

Internal audit teams build their audit plans on a number of factors, among them the organization's overall risk appetite. Auditors consider the organization's financial risk limits and appetite statements, as well as considerations such as laws and regulations, organizational policies and standards, and the expectations of stakeholders-such as the board, investors, analysts, customers, employees, and business partners—as well as industry standards.

One step for boards is to see that internal audit has a chance to play a critical role in ensuring the completeness and accuracy of non-financial data. Unfortunately, many organizations are not making full use of the contribution that internal audit can make. The chief audit executive (CAE) reports to the board on ESG issues at only 11% of public companies surveyed and 8% of private companies, according to the NACD survey.

Internal audit can provide data and advice that can help mitigate and identify risks that include:

- **Impact on the business model.** Companies may find themselves facing unexpected pressure to adopt new practices that address unexpected non-financial risks.
- **Loss of competitive edge.** Non-financial risks have the potential to damage a company's market share and reputation.
- **Difficulty accessing capital or higher borrowing costs.** Investors or lenders may require greater transparency on non-financial risks than the company can offer.
- **Labor disadvantages.** A tight hiring market or lack of employee engagement could be damaging, particularly if a company appears as an unappealing place to work.
- **Social and geopolitical implications.** Companies may fail to anticipate localized social or civil unrest.

A Deep Understanding

"Risk management cannot be seen as a collection of static practices but must evolve to keep pace with rapidly changing business models," according to a McKinsey report.[9] As companies monitor and maintain risk approaches for non-financial data, internal audit can provide a deep understanding of the organization and ongoing insights in a changing and uncertain risk landscape.

QUESTIONS FOR BOARD MEMBERS

» Are non-financial risks incorporated into our organization's risk appetite?

» How does our organization monitor non-financial risk?

» What controls are in place to identify, prevent or mitigate non-financial risks?

» Are these controls regularly evaluated and updated?

» Is the board receiving independent assurance from internal audit on non-financial risk measurement and oversight?

Quick Poll Question

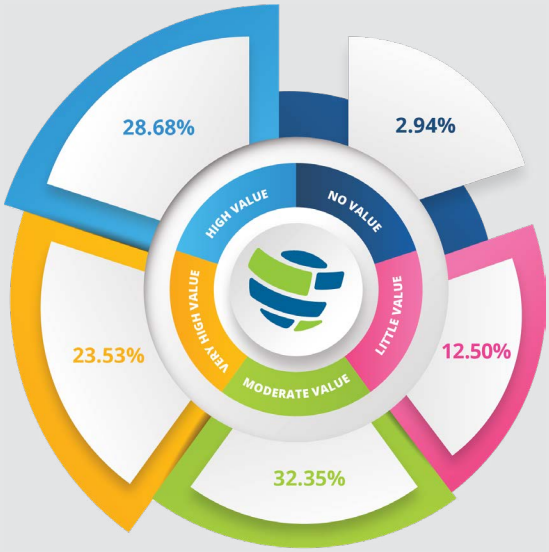
Are non-financial risks incorporated into your organization's risk appetite?

- ◯ Yes
- ◯ No
- ◯ Don't Know

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

QUICK POLL RESULTS

Overall, how would you rate the value that has been created from internal audit's use of data analytics or automation at your organization?



Source: Tone at the Top December 2022 Quick Poll Survey.

[1] "Taking Control: How to Get on Top of Non-Financial Risk," Christopher Eaton and David O'Brien, PwC, March 9, 2021.

[2] 2022 NACD Board Practices and Oversight Survey—ESG: Compare and Contrast Among Public and Private Companies, NACD, 2022.

[3] https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf

[4] "ESG and Stakeholder Capitalism," Andrew Droste, Russell Reynolds Associations, published by Bloomberg Law, April 2020.

[5] "SEC Proposes Rules to Enhance and Standardize Climate-Related Disclosures for Investors," US Securities and Exchange Commission press release, March 21, 2022.

[6] "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," SEC press release, March 9, 2022.

[7] "Emerging Fraud Risks to Consider: ESG; On the Audit Committee's Agenda," Deloitte, July 2022.

[8] 2022 NACD Board Practices and Oversight Survey—ESG: Compare and Contrast Among Public and Private Companies, NACD, 2022.

[9] "Financial Institutions and Nonfinancial Risk: How Corporates Build Resilience," Bjorn Nilsson, Thomas Poppensieker, Sebastian Schneider, and Michael Thun, McKinsey, February 28, 2022.