GLOBAL KNOWLEDGE BRIEF

Governance, Risk, and Control

Part 1: Rethinking Risk Appetite from a Non-Financial Risk Perspective

The Institute of Internal Auditors

Contents

About the Expert

W. Scott Page, CIA, CCSA, CRMA, CPA, CA

Scott is director of internal audit at MDA, Ltd. Based in Brampton, Ontario, Canada, MDA provides geo-intelligence, robotics, and space operations and satellite systems. Scott has more than 20 years of expertise in defense and space manufacturing, professional services, healthcare, distribution services, and manufacturing industries.

Introduction

The concept of risk appetite — the amount of risk that an organization is prepared to accept to achieve its objectives — is fundamental to effective governance in all organizations. Historically, decisions about a company's risk appetite were governed primarily by financial risk considerations. That is changing, however, amid a growing focus on non-financial risks, including environmental, social, and governance (ESG) risks and related regulatory and reporting considerations. Increasingly, more attention is being paid to risks associated with how organizations operate in relation to the world around them.

Assessing these risks as part of the risk appetite is an area where internal auditors can make meaningful contributions. This Global Knowledge Brief, the first in a three-part series on governance, risk, and control (GRC) from The IIA, examines in detail this topic, the challenges of rethinking risk appetite with non-financial risk in mind, and the important role of internal audit in the process.

The Risk Appetite

Balancing threats and opportunities

Risk profiles impact appetite

The IIA's International Professional Practice Framework defines risk appetite simply as, "The level of risk that an organization is willing to accept." In practice, risk appetite, also referred to as risk tolerance, represents a balance between the potential benefits of innovation and the threats that change inevitably brings. As such, risk appetites are unique to each organization and vary depending on any number of factors, such as:

Culture — Based on long-standing guidelines, attitudes, or other factors, the organization may be more or less aggressive in its approach to risk.

Industry — The amount of regulation or other compliance concerns, for example, may have an impact on how risk averse it is.

Market — The level of competition a company faces or the stability of its market are factors that can affect decision making on risk.

Financial strength — A company that is less confident in its financial position may be more risk averse[1].

What is non-financial risk?

Incorporating non-financial risk into discussions on risk appetite begins with understanding what it can encompass. Indeed, the sheer number of risks that fall into this category (see related list) increases the chances that some may be overlooked or misunderstood, which underscores the importance of incorporating non-financial risks into any discussion on risk appetite. Beyond simply incorporation, however, organizations must also be prepared to act on these non-financial elements, identifying the information necessary to address risk within different business processes at the corporate level,

NON-FINANCIAL RISKS
(partial list)

- Operational
- Compliance
- Strategic
- Third-party
- Cybersecurity
- Social responsibility
- Reputational
- Data privacy
- Data integrity
- Intellectual property protection
- Compensation
- Employee conduct
- Labor management
- Ethical and corporate culture
- Public health
- Diversity, equity, and inclusion
- Human rights
- Human resources
- Environmental:
  - Greenhouse gas emissions
  - Waste management
  - Raw material sourcing
  - Natural resources access/management
  - Climate change

[1] Jean-Gregoire Manoukian, "Risk Appetite and Risk Tolerance: What's the Difference?", Wolters Kluwer, September 29, 2016, https://www.wolterskluwer.com/en/expert-insights/risk-appetite-and-risk-tolerance-whats-the-difference#:~:text=Risk%20Appetite%20Is%20the%20General%20Level%20of%20Risk%20You%20Accept&text=Because%20determining%20risk%20appetite%20will,risk%20you%20need%20to%20manage.

Challenges related to reporting on non-financial risk

Reporting

More than 60% of CAEs at publicly traded organizations considered sustainability/non-financial reporting risk levels to be moderate, high, or very high, according to The IIA's *2023 North American Pulse of Internal Audit*.[2] Indeed, many companies are working to measure and report on sustainability/non-financial issues. For example, a total of 96% of companies listed on the S&P 500 and 81% listed on the Russell 1000 publish sustainability reports.[3]

One challenge for organizations in this area is that many non-financial risks are difficult to measure. Examples include inclusion, ethical behavior, corporate culture, and the environmental impact of actions taken by the company and its suppliers and business partners.[4] A related concern involves potential fallout if organizations rely on incorrect or misleading indicators or frameworks in aggregating or reporting non-financial information.

There are currently no definitive, globally embraced standards on non-financial reporting and disclosure, which can lead to a lack of consistent and comparable reporting. Instead, organizations generally have the opportunity to pick one set of guidelines, to pull together different guidelines, or to opt out of reporting completely based on their needs. Indeed, the Center for Sustainable Organizations compiled a list of 23 non-financial measurement and reporting standards and frameworks that address a variety of different constituencies, performance constructs, and primary measurement formats.[5]

However, a set of more generally accepted reporting standards are on the horizon. One important development was the creation of the International Sustainability Standards Board (ISSB) by the International Financial Reporting Standards Foundation (IFRS) Foundation. It consolidates the existing Value Reporting Foundation and Climate Disclosure Standards Board and has taken on responsibility for the Integrated Reporting Framework, all part of an effort to create a comprehensive global baseline of sustainability disclosure for the capital markets. Its goal is to meet demands for high-quality, transparent, reliable, and comparable reporting by companies on climate and other ESG matters. The ISSB announced that its initial standards on climate and sustainability reporting will be issued towards the end of Q2 2023.

Regulatory

According to the World Business Council for Sustainable Development (WBCSD), there currently exist more than 2,000 mandatory and voluntary ESG reporting requirements and resources from across more than 70 countries. This alone creates a daunting challenge for organizations trying to understand mandatory and voluntary non-financial reporting and related risks.

The European Union (EU) has taken the lead on mandatory disclosure of non-financial risk. Since 2014, the Non-Financial Reporting Directive (NFRD) required large public-interest EU-based companies with more than 500 employees (approximately 11,700) to publish information related to environmental matters, social matters, treatment of employees, respect for human rights, anti-corruption and bribery, and diversity on company boards (in terms of age, gender, education, and professional background), among other matters.

In January 2023, the EU's Corporate Sustainability Reporting Directive (CSRD) went into effect. It updates social and environmental reporting rules under the NFRD and expands the number of companies required to report (approximately

---

2. *2023 North American Pulse of Internal Audit*, The IIA, 2023, https://www.theiia.org/globalassets/site/content/research/pulse/2023/2023-Pulse-of-Internal-Audit.pdf.
3. *2022 S&P 500 and Russell 1000 Sustainability Reporting in Focus*, Governance & Accountability Institute Inc., 2022, https://www.ga-institute.com/research/ga-research-directory/sustainability-reporting-trends/2022-sustainability-reporting-in-focus.html#:~:text=All%2DTime%20High%20of%20Sustainability,and%2081%25%20of%20Russell%201000.
4. *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA,, May 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.
5. "Non-Financial Measurement & Reporting Standards & Frameworks," Center for Sustainable Organizations, 2023, https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf.

50,000). Companies will have to apply the new rules for the first time in financial year 2024 for reports publishing in 2025. Until then, the NFRD reporting rules apply.[6]

In the U.S., the Securities and Exchange Commission (SEC) has proposed requiring registrants to include specified climate-related and cybersecurity disclosures in their registration statements and periodic reports. The SEC is expected to announce final rules in these two areas in 2023. Although exempt from any SEC requirements, private companies may also feel pressure from stakeholders to make similar disclosures.

Greenwashing

In addition to a lack of comparability and transparency in reporting, trustworthiness can become a problem when companies use overly optimistic assumptions in setting targets or when they misrepresent data to present a more positive picture. In Europe, national consumer protection authorities found reason to believe that 42% of green-friendly claims by businesses were exaggerated, false, or deceptive. These practices, known as greenwashing, can damage organizations' reputations. The resulting impact on customer satisfaction with a company and its products or services can influence earnings per share and return on investment.[7]

In addition, according to The IIA, "without a reasoned ESG risk management strategy built on a clear-eyed understanding of the issues, poorly executed sustainability reports can quickly run afoul of regulatory compliance and astray of investor expectations."[8]

42

PERCENTAGE OF GREEN-FRIENDLY CLAIMS BY BUSINESSES BELIEVED TO BE EXAGGERATED, FALSE, OR DECEPTIVE.

Source: Harvard Business Review, *"How Greenwashing Affects the Bottom Line"*

Companies grappling with non-financial data for the first time will have to develop new key performance indicators and other metrics, along with appropriate policies, processes, and internal control measures to generate reliable information for decision-making and ensure the quality of data being produced and reported.

6. "Corporate Sustainability Reporting," European Commission, accessed March 2023, https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en.
7. Ioannis Ioannou, George Kassinis, and Giorgos Papagiannakis, "How Greenwashing Affects the Bottom Line," July 21, 2022, Harvard Business Review, https://hbr.org/2022/07/how-greenwashing-affects-the-bottom-line.
8. *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA, May 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.

Considering non-financial risks in audit planning

Internal auditors plan their audits based on the risk appetites of the overall organization and the areas being audited. Internal audit is often given responsibility for providing independent assurance on the effectiveness of an organization's risk appetite framework. The growing regulatory and stakeholder focus on sustainability and other non-financial issues demands that internal audit leaders consider related risks that may pose a threat to the organization, including understanding how they fit into the company's activities and strategies and knowing which departments have oversight of related practices. Internal audit leaders also should raise awareness about non-financial risks with boards and executive management.

One key role for internal audit will be to determine an appropriate control environment for non-financial risks that can monitor relevant measures and prevent an organization from reporting invalid and misleading information because of poorly designed controls and systems. Competent internal audit functions have the skills and experience necessary to support effective non-financial control environments, including training and advisory services. Internal audit can advise on frameworks or standards the organization can use to manage, mitigate, and possibly report on non-financial risks. Internal audit also can offer advice on the most useful reporting metrics, including new indicators designed to capture both quantitative and qualitative data that accurately represent non-financial risks.

Data suggest that sustainability and non-financial considerations are slowly working their way into internal audit's routine. According to the Pulse report, 22% of respondents said they incorporate sustainability considerations in their audits generally. However, specific audits of sustainability/non-financial reporting made up a scant 2% of audit plan allocation.[9]

The value of a centralized focus: one company's experience

Setting the proper foundation is an important factor in incorporating non-financial risks into the risk appetite.

When Scott Page joined MDA, Ltd. as director of internal audit, each business area had its own risk management process, but the company was interested in centralizing its focus. To achieve that centralization, a holistic and integrated approach was key. To bring information together, the Canada-based public company, which provides services in robotics, satellite systems, and geo-intelligence, adopted a versatile software tool for the assessment process. The same tool can be used by other teams, including internal audit in control testing and IT in assessing cyber and third-party risks.

Risk information and controls are thus shared across the company. The tool gathers details on all the risks that might impact strategy or objectives to see how they might affect the company's ability to deliver on its short-term objectives, as well as its long-term strategic plan. "We wanted to pull all the risk considerations together in a single source of truth," Page said. "It helps us to understand how what we do interrelates with everyone else."

Risks related to internal controls, financial statements, operations, IT, and third parties were already well captured using current approaches. However, the organization has also begun considering ESG and other non-financial risks. Using the

9. *2023 North American Pulse of Internal Audit*, The IIA.

same tool to consolidate these additional risks means that “you’re always informed of what’s going on in other areas,” Page said.

While identifying, accounting for, and auditing non-financial risks can be complicated, MDA’s centralized focus has given it a solid starting point. Among other concerns, the company doesn’t want to separate ESG into a silo, because the related non-financial risks touch on so many areas.

Centralization enables use of a common language that can be understood across the company and by stakeholders, said Page. He, along with leaders in the enterprise risk management (ERM) group, define risks and how they should be evaluated on a scale of 1 to 5. Risk information can be collected once and leveraged across the organization, enhancing efficiency in internal audit and elsewhere, as well as ensuring version control. Using that common language, executive management and the board can easily understand when internal audit or other teams designate a risk as a top priority — Category 5 — as opposed to a less urgent priority — Category 1.

One ongoing consideration is the auditability of non-financial information, because there are, as previously discussed, no generally adopted reporting standards. Until this changes, internal audit can provide advice on what controls, processes, and information an organization will need to be prepared for.

Quantifying the numbers is another challenge, because data may not be available, and comparable data may be difficult to obtain. MDA, for example, doesn’t have much in the way of greenhouse gas emissions itself, one common ESG concern. However, it does work with many outside vendors and consultants, and those third parties could be creating emissions or taking other steps that MDA will need to consider. In developing the pillars of its non-financial risk program, MDA is identifying those third parties, considering how to measure any related risks, deciding how best to audit them, then developing a broader understanding of what third-party and other non-financial risks mean for the company.

According to The IIA’s Pulse survey, third-party relationships are the third highest risk area (after cybersecurity and IT), and audit frequency for third-party relationships is relatively low compared to risk level.

Even though MDA is in the early stages of identifying areas of potential non-financial risks, the process so far has highlighted how much impact they could have on the company’s ability to achieve its strategies, as well as on the public’s perception of the company. The process will also provide more information for decision making to executive management and the public, Page said. “We have a fuller understanding of both financial and non-financial risks and how we need to control them,” he stated.

Being involved from the outset

Internal auditors should alert management and boards to the value of including internal audit from the start, especially when tackling a new concept such as non-financial risk. “If internal audit is involved up front, there is a better chance for success down the road,” said Page. “Why should a company roll out its ESG or non-financial plans or processes, then have internal audit come in later and point out all the problems with it once it’s in place?”

To maintain independence, internal audit cannot be in a position of making decisions for a company, but it can offer insights on the best way to get started in considering non-financial risks and what approaches might or might not work. “We can be a value-added business partner,” he said.

Page has found that making contacts throughout the organization is a good way to better understand the areas his team will be auditing. Page regularly contacts people involved in important business functions and asks for a 15-minute meeting over coffee — and he encourages his staff to do the same. “No one has ever said no,” he said. “They are all passionate and love what they do.”

“What concerns me as head of audit is: What don’t I know?” Page added. “The only way to find out is by talking to people.” His team’s audits include conversations with staff of the area being audited. He also keeps up to date on the work of the corporate ERM team, although internal audit has its own independent risk assessment process.

Networking with his peers on industry or professional committees also helps to determine if his risk management approach is up to date and as thorough as it can be. This background knowledge will be especially important for non-financial or ESG information as these risks continue to evolve.

Page and his team have come away from their conversations with greater understanding and are, therefore, better positioned when it comes time to audit an area, something that will be particularly useful in understanding the new frontier of non-financial data. MDA encompasses three separate business areas, so internal audit can also share successful practices used by other teams and spot unnecessary duplication of effort. “Business acumen leads to much greater success,” Page said. Internal auditors can provide value, as well, by challenging the status quo, questioning existing practices, and developing guidelines to enable better understanding and identification of non-financial information.

Practical direction from *Risk in Focus 2023*

Risk in Focus 2023, the latest annual report on risk produced by members of the European Confederation of Institutes of Internal Auditing (ECIIA), addressed various non-financial risk areas, including macroeconomic and geopolitical risks. Participants in a roundtable of internal audit leaders addressed reassessing global risk, particularly as the conflict in Ukraine has impacted risks in various areas, including the stability of global energy systems. One roundtable participant, Ken Marnoch, executive vice president, internal audit and investigations at Shell International, said he and his team are engaging in "stronger conversations about risk appetite."

From *Risk in Focus 2023*:

> "[Marnoch] says having a clear understanding of how much risk each business can take on in specific areas is most useful during a dilemma — where all choices may have potential upsides and downsides. Then, clarity on the appetite for the risks associated with the different choices can act as a guiding light through the problem.
>
> Historically, Shell's internal audit had focused on operational, culture, and conduct-based risks. The internal audit group has now set up a specific team to focus on the risks and control framework associated with the delivery of strategic objectives.
>
> 'If you break strategic objectives down to measurable goals, the related risks, the explicit controls, and an understanding of how business leaders know that the controls are working, then you have the scope for an internal audit,' he says. 'Part of the role of the new team is to help people move away from fixed thinking around the correctness of assumptions they made at the beginning of a project, or strategy, when so much in the world is changing dramatically. How to be actively inquisitive, to find information that tests the beliefs and the fast feedback on the current reality are required to navigate an uncertain future.
>
> 'If you let go of the need to be right and acknowledge it was a decision made with the best information at the time, you will be more open to looking for information that challenges your thinking. That opens up a lot more power in managing a key risk in the delivery of your strategic objectives.'"[10]

Risk in Focus 2023 includes a list of questions internal audit can use in evaluating organizational risk:

1. In terms of the time and effort spent on internal auditing assignments, how is internal audit aligned to the organization's strategic objectives — including those involving geopolitical risk and climate change?
2. How strong is the support for internal audit activities in areas such as strategy and crisis management and what can be done to improve that support where it is lacking?
3. How far is internal audit able to leverage resources of other lines to provide proper coverage and minimize duplication of effort?
4. How do you know whether the assumptions the organization (and the internal audit function) have made about the nature of key risk areas are still valid today and fit the circumstances likely to arise in 2023?
5. Does the organization have up-to-date risk assessments for sanctions risk and robust controls for screening third-party ownership and company shareholders?
6. How far does the organization take advantage of digital tools to model key risks and to run "what if" scenarios?
7. Have you reassessed the relationship between the organization's business continuity, crisis management, and risk management teams to ensure they are fit for purpose?
8. Does the organization seriously consider critical voices and those of external experts in their assessment of risks?

[10] *Risk in Focus 2023: More Risky, Uncertain, and Volatile Times Ahead,* European Confederation of Institutes of Internal Auditing, 2022, https://www.eciia.eu/2022/09/risk-in-focus-2023-more-risky-uncertain-and-volatile-times-ahead/.

Conclusion

A comprehensive understanding

It is important to understand that non-financial risks can have a meaningful financial impact on an organization, including its ERM efforts. To help leadership understand and tackle non-financial risks, internal audit leaders can use their comprehensive understanding of the entity's many facets — and threats — to provide valuable insights on these risks, as well as to appropriately account for and address them when helping to determine the organization's risk appetite.

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.

Disclaimer

Copyright

April 2023

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101