GLOBAL KNOWLEDGE BRIEF

Governance, Risk, and Control

Part 2: Quantifying Non-Financial Risk

The Institute of Internal Auditors

Contents

About the Expert

Anishka Collie, CIA, CPA

Anishka Collie, CIA, CPA, is CEO and principal consultant at ATC Financial Advisors & Consultants, in Nassau, the Bahamas. She has over 20 years of experience in external auditing, internal audit and corporate governance, enterprise risk management and internal controls, as well as in financial planning, consulting, financial process remediation, and business process reviews. She focuses on clients in the financial services industry and has presented at numerous accounting and auditing training seminars.

Hassan NK Khayal, CIA, MBA, CRMA, CFE

Hassan NK Khayal, CIA, MBA, CRMA, CFE, is an internal audit manager at Scope Investment in Dubai. He was featured as one of the top 15 under 30 global Emerging Leaders as an up-and-coming star of the internal audit profession in Internal Auditor, a global publication of The Institute of Internal Auditors. He is completing his doctorate in business administration at Catholic University in Murcia, Spain. In addition to his degrees and professional certifications, he also holds professional certifications in robotic process automation, quality management, health and safety, environmental management, and risk management.

Jason Minard, CIA, CISA, CPA (inactive)

Jason Minard, CIA, CISA, CPA (inactive), is a senior vice president and senior manager of Supervisory Controls and Analytics at Wells Fargo Advisors, in St. Louis, Missouri, USA. With over 25 years of experience in the securities industry and audit, he has performed and managed audits in areas such as investment sales, regulatory compliance, securities operations, investment banking, asset management, trust administration and finance. He has a bachelor's degree in business administration from St. Louis University and holds general securities representative and general sales supervisor licenses.

INTRODUCTION

Management guru Peter Drucker is often quoted as saying, "[only] what gets measured, gets managed." Indeed, companies have long understood the importance of quantifying and measuring financial risks. The new wrinkle in recent years has been the rising interest in non-financial risks, including environmental, social and governance (ESG), and related regulatory and reporting considerations. The challenge has been how to measure something that often has no easily identified monetary value. It is one that organizations must overcome, because non-financial risks can definitely have a financial impact.

This Global Knowledge Brief, the second in a three-part series on governance, risk, and control (GRC), examines the challenges of quantifying non-financial risks and how companies are addressing them, as well as the important role that internal audit can play in advancing understanding in this area.

UNDERSTANDING NON-FINANCIAL RISKS

Myriad potential threats

Learning How to Recognize and Measure

As a general rule, non-financial risks are those that arise from an organization's impact on the world, and, conversely, the world's impact on the organization. A partial list (see box) reflects many but not all the wide range of non-financial risks organizations may face. The definitions of these risks are often inconsistent or unclear, making recognition and measurement more challenging.

However, non-financial risks also exist in straightforward financial transactions. For example, in considering credit risk on a $50,000 loan, the loan value and the potential initial loss are clear. On the other hand, non-financial risk for this transaction includes considerations such as the time and effort spent dealing with a potential loan default, noted Anishka Collie, CIA, CPA, CEO and principal consultant at ATC Financial Advisors & Consultants, Nassau, the Bahamas, which provides outsourced risk and internal audit advisory services. If the loan is significant or part of a pattern of bad loans, the organization may also have to dig deeper to understand if the corporate culture, the available documentation and internal controls, or the current training level are appropriate to mitigate credit risk and ensure good lending decisions.

Because non-financial risks can be difficult to quantify, a related risk is the possibility that an organization's reporting and disclosure of non-financial risks are unreliable. For example, achievement of certain sustainability goals may be viewed as intentionally inflated or that problems reaching those goals are understated, a practice known as greenwashing when it's related to ESG issues. Greenwashing may be intentional, or it may simply occur because of the relatively low levels of maturity currently available in non-financial reporting standards, noted a chief audit executive at a roundtable held by the European Confederation of Institutes of Internal Auditing (ECIIA).[1] At the moment, reporting may be inconsistent or difficult to compare because there are no globally embraced standards on non-financial reporting and disclosure. There are also various frameworks or standards available, making it potentially difficult for companies to determine which guidelines to follow and how to apply them, particularly because they often may be used in part or in combination with rules from

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] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.

another standard or framework. The Center for Sustainable Organizations compiled a list of 23 non-financial measurement and reporting standards and frameworks that are based on numerous different performance measures and aimed at different types of organizations.[2]

Setting the Stage

Organizations should be proactive in considering how to quantify non-financial risk, but many are not. Dealing with financial risk correlates with an organization's main goal — maximizing shareholder wealth and enhancing revenues. In addressing non-financial risks, organizations are asked to spend money on efforts whose value can be hard to understand and that don't immediately add to revenue. "Until you can quantify and put a financial figure on the impact of the risk, you're unlikely to secure the required management buy-in to address it," according to PwC.[3]

Another hurdle is that control functions for non-financial risks can be siloed throughout an organization. Because these risks are so diverse, they often are under the oversight of a wide range of teams. Each team may have its own risk identification process, reporting structure, and even different IT systems related to non-financial risks. "The same individuals, whether internal audit, compliance, or some other area, are being asked to do the same procedure over and over again," said Hassan NK Khayal, CIA, MBA, CRMA, CFE, internal audit manager at Scope Investment in Dubai. The added expense of this duplication of effort makes it more likely that management may push back on investments in information gathering and quantification efforts.

However, taking preventive measures lowers remediation costs and protects the company's brand and business relationships. At most organizations, risk reporting methods are not yet sophisticated or precise enough to make a compelling case to management, Khayal said. But if selected appropriately, the right indicators can capture and accurately quantify non-financial risks and provide the proper context for management to grasp their potential impacts.

Proactively identifying potential non-financial threats before they happen makes it easier to understand and quantify them. For example, in the food and beverage industry, it's easy to quantify the financial risk when a certain amount of food is spoiled. However, calculating related health and safety costs and risks is harder, Khayal noted. By considering these risks an organization can take proactive, preparatory steps, such as enhancing cleanliness to make a restaurant more appealing and less likely to cause customer illness. Similarly, in the construction industry, when safety engineers are more stringent in monitoring and enforcing health and safety rules, the number of accidents typically drops.

"Each incident comes with its own associated cost," Khayal said, whether it is the direct cost of dealing with the event and any related injuries, or the expense of associated delays. "The moment the risk has occurred, it's already too late," he noted, and the damage to the organization's reputation and relationships has been done, perhaps with lasting or significant impact. But when organizations evaluate the costs of potential risk events, they are more likely to see the value of taking preventive measures.

Khayal believes that non-financial risks can have greater effects than financial ones. Their impact may leave stakeholders such as shareholders, employees, and customers questioning a company's business model or practices when reputational damage occurs. "All of this puts considerable pressure on organizations to manage non-financial risks," he said.

Working Toward Quantification

While non-financial risks don't carry direct monetary values, it is possible to assign them numerical values. The key is to define the risks and what they encompass, then find tangible considerations to measure. In addressing customer risk, for example, it's possible to determine factors such as the number of customer complaints, the related locations or situations, associated customer losses, declines in new customers, and what trends this data reveal over time.

[2] https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf
[3] "Taking Control: How to Get on top of Non-Financial Risks," Christopher Eaton and David O'Brien, PwC Channel Islands, March 9, 2021.

When there are no tangible criteria to measure, one option is to categorize risks in a way that is as descriptive and meaningful as possible, such as whether they are at high, medium, or low levels. For example, when there is a compliance and regulatory risk, organizations might try to quantify risk by determining the range of potential findings from a regulator in each risk category. Categorizing findings this way gives companies a framework for further assessing each risk and setting priorities.

An organized ratings framework is another option that makes it possible to capture findings on a range of non-financial risks. Internal audit teams might use a ratings framework that rates observations made by internal audit and any other teams, such as compliance, risk, information security, or legal, that identify unmitigated risks and track, report or remediate them. The framework can be used to assess the impact of non-financial risks and support quantification of them. One example of the type of framework companies might use to better understand and communicate the financial impact of their sustainability measures is the United Nations Global Compact and Principles for Responsible Investment Value Driver Model.

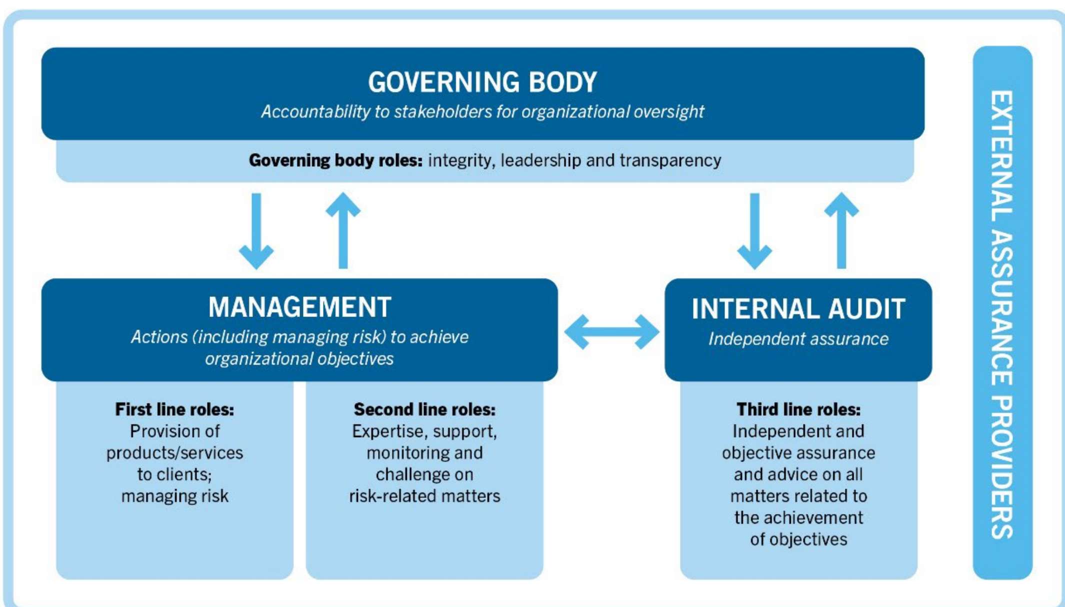
THE ROLE OF INTERNAL AUDIT

Non-Financial Risk "Pioneers"

Remaining Future-focused and Monitoring Controls

As companies work to address quantification, the role of internal audit is to be strategic and focus on the best ways to add value, as described in The IIA's Three Lines Model (See Figure 1). To achieve this goal, internal auditors should not confine themselves to analyzing statements and financial risks, but rather they should be the pioneers in addressing non-financial risks by following a risk-based approach and always considering the future, Khayal said. "Ideally, we should be one of the more future oriented departments in the organization," he said. "We should focus on future risks before management, with its eye on day-to-day impacts, is even aware of them." To maintain independence, internal audit doesn't define the risk categories or definitions the organization uses, but it does challenge non-financial risk policies and how they are implemented in line with the overall risk assessment process.

Figure 1: Three Lines Model



As a consultant, Collie's role is much like that of an internal auditor and is one that auditors can follow when it comes to non-financial risks. At the outset, she speaks with organization leaders, including not only the CEO and CFO but also the heads of compliance, risk, and internal audit. The goal is to understand their definitions of risk for their organization, how they identify risks, at what level of detail, and what controls are in place. During these discussions, participants often come to a new understanding of risk and its impact, Collie said.

These initial conversations are high level to understand what is required for the organization to operate effectively. The next step is to talk to managers or heads of departments to learn more about day-to-day operations and where risks may occur. With that understanding, the auditor can brainstorm with employees at this level to learn what risk management steps have already succeeded or failed and where risk management weaknesses exist. Just as consultants can offer experience with a variety of organizations, internal auditors have a holistic knowledge of many areas of the organization. “You can bring things to surface these teams may not have thought of,” Collie said.

Auditors will need new skills to facilitate the process. Traditional internal audit approaches involve identifying risk as it relates to controls, data, and documents. Working with clients to identify and understand non-financial risks requires additional skills and ongoing training related to interviews or facilitating a brainstorming session, Collie said. “Actually helping clients walk through the process of identifying risk is a completely different exercise,” she said. Leadership will have to invest in this education to ensure the organization is performing in an effective and efficient manner.

Internal audit can also assess the value and reliability of existing key performance indicators and metrics when applied to non-financial risks, as well as new measures developed specifically for non-financial risks and related controls and risk management processes. To prevent charges of greenwashing, they can ensure that the data shared with stakeholders paints a fair and accurate picture of corporate efforts, according to the ECIIA.[4]

Khayal builds his audit plan and risk assessment around the many risk elements that can affect an organization’s ability to achieve strategy, both financial and non-financial. For example, if organizational strategy and value creation depend on rigorous supply chain practices, then procurement would always be a key concern, he said. Mapping risks, and particularly non-financial risks, can reveal threats such as customer creditworthiness problems, supply chain issues, and cybersecurity challenges.

As organizations build out their frameworks and refine the definitions they use, they create a common language about non-financial risks. That enhances communication about risk among the first, second and third lines; clarifies responsibilities for each line; and allows each to add its own refinements to the shared definitions.

Future-facing Responsibilities

At Khayal’s organization, anyone involved in controls and risk self-assessment must take a detailed risk training course that includes non-financial risk. He also encourages his staff to focus on three key tasks:

- **Stay up to date**. Internal auditors must keep abreast of the latest world and local events to gain a better understanding of incidents that could have an impact on risk now or over the near or long term.
- **Keep current on emerging technologies.** Khayal believes the auditors of the future and the organizations they work for must be IT savvy. Auditors can no longer rely solely on traditional methods but must incorporate technology tools. “The world is changing at a more rapid pace,” he said. Without robust technology, “organizations will not be able to keep up, especially as more and more macroeconomic factors that we’re facing are non-financial.”
- **Remain in tune with organizational strategy, mission, and vision.** Audit plans must consider which risks matter most and how best to quantify them. Because organizations generally can’t address every type of risk they may face, auditors must take various factors into account to identify and attempt to quantify those risks likely to have the greatest importance and impact.

[4] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.

CONCLUSION

As the organization's trusted advisers, internal auditors are in a unique position to drive greater understanding and recognition of non-financial risks. They can do so by harnessing their existing comprehensive knowledge of the business, adding new competencies, and advocating for a change in organizational perspective that determines how best to quantify non-financial risk.

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

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

May 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