GLOBAL PERSPECTIVES & INSIGHTS

Governance, Risk and Control

PART I: Rethinking Risk Appetite from a Non-Financial Risk Perspective

PART II: Quantifying Non-Financial Risk

PART III: How Digital Transformation Is Transforming GRC

The Institute of Internal Auditors

Contents

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

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 50,000). Companies will

---

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.

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.

The Role of Internal Audit

Assurance and advisory services

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."

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

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 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.

Part 2: Quantifying Non-Financial Risk

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).[11] 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 another standard or framework. The Center for Sustainable Organizations compiled a list

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

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

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.[12]

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.[13]

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.

[12] https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf
[13] "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.

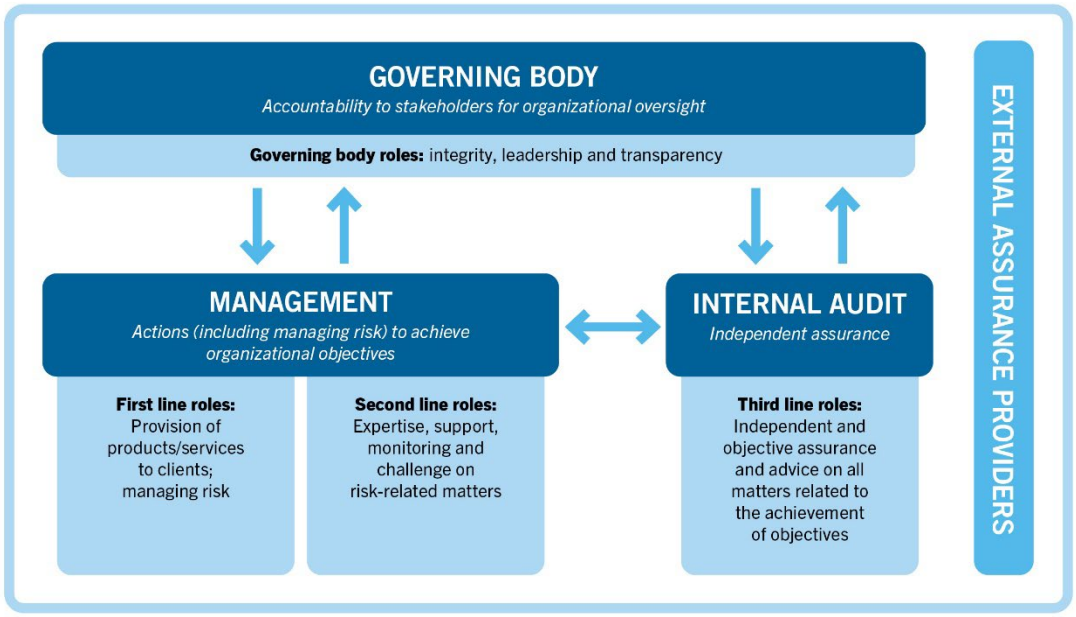
THE ROLE OF INTERNAL AUDIT

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.[14]

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.

[14] *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.

Part 3: How Digital Transformation Is Transforming GRC

About the Experts

Sarah Kuhn, CIA, CCSA, CRMA

Sarah Kuhn is a highly experienced professional in the field of internal audit. With over 20 years of membership in The Institute of Internal Auditors (IIA) and a past presidency of the Tulsa chapter, she has demonstrated her commitment to the industry with experience in department training, reporting, and standards compliance, as well as leading an audit team focused on analytics and automation. Sarah also currently works as an officer in The IIA Houston Chapter.

Audra Nariunaite, CIA, CISA, CFE, CHC, CHPC

Audra Nariunaite is a compliance and audit professional with multi-industry experience and a proven ability to drive growth and excellence through strategic initiatives and process reengineering. She currently serves on the board of directors for The IIA Northeast Florida Chapter and is a member of IIA–Lithuania. Audra is presently a director of compliance at global employment platform Oyster HR.

Introduction

Arguably, no trend is affecting the governance, risk, and compliance (GRC) landscape more significantly than the rise of technologies in daily business operations — and it is easy to see why. The benefits of digital transformation cannot be understated, with tools springing from this trend now being used across nearly every major industry to automate and accelerate processes, allowing GRC and security operations to quickly identify and respond to potential risks and issues.

For example, with its ability to analyze unstructured data sources ranging from emails to social media feeds, AI-assisted natural language processing can be combined with the skills and experience of human GRC teams to provide risk and compliance management resources at a level of sophistication and complexity that could not have been fathomed just a generation ago.

While the need to undergo such a radical digital transformation might have once been considered a luxury, today's risk landscape provides organizations little room for delaying adoption. Cyberthreats are intensifying in volume and sophistication by the day; the raw volume of data being produced, collected, and processed continues to grow at a staggering rate, creating ever-increasing data privacy risks; and the regulatory landscape continues to evolve rapidly to match the speed of today's risks. Indeed, without the advantages digital transformation provides, GRC functions in today's world might well be lost.

As Part 3 of The IIA's Global Knowledge Brief series on GRC, this final installment addresses how GRC systems are evolving from the incorporation of new technologies as well as what inherent risks are involved in embracing digital transformation. This brief also addresses where internal audit fits into this conversation and how it might best aid organizations as they continue this critical journey.

The 2023 Digital Transformation Conversation

Understanding a loaded risk

The scope of digital transformation

The digital transformation explosion seen during the COVID-19 pandemic continues to rage, and in some ways its evolution is gaining speed. This has occurred not only because of a baseline desire to increase profits and efficiencies to gain a competitive edge in the marketplace, but also because of a drive to maintain pace with (or, ideally, get ahead of) the extensive list of emerging risks that have materialized in recent years. Inflation, geopolitical tensions such as the Ukraine conflict, the China-Taiwan dispute, widespread economic uncertainty resulting from events such as the sudden closures of numerous large-scale banking institutions, ongoing discussions pertaining to ESG risks and related changes to the regulatory landscape, supply chain disruptions and shortages — these are just a few of the forms risk has taken in 2023. From the perspective of organizations tasked with maintaining some semblance of assurance against them, a wide-scale embrace of digital transformation is viewed as an effective salve. Indeed, according to a recent report from Gartner, 89% of board directors say that digital business is now embedded in all business growth strategies, even if just 35% say they have achieved or are on track to achieving digital transformation goals.

"Boards of directors have reached a point where digital business strategy and overall business strategy are one and the same," said Jorge Lopez, VP and distinguished analyst at Gartner, in the report. "While CIOs have made significant progress leveraging technology for operational excellence, this is not enough to realize the strategic business benefits that [boards of directors] are looking for from digital investments."[15]

What digital transformation looks like varies from location to location, industry to industry, and organization to organization. What is effective, or even achievable, by one organization may not be ideal for another. Despite this, there are some fundamental similarities among organizations embracing some form of digital transformation. "[Digital transformation] is about more than just technology," said Chintan Shah, CEO and founder of Brainvire, writing for *Forbes*. "[I]t's about the shift in mindset that enables organizations to reimagine their business models and processes to take advantage of the opportunities created by emerging technologies."[16]

Lopez expressed a similar sentiment. "As enterprises increasingly operate in a world of constant disruption, the most future-savvy boards are considering how upheavals and risks can serve as a source of opportunity. CEOs and CIOs will need to adopt this mindset as technology plays an ever-expanding role in driving business success."

Such reimagining can take many forms, including, but not limited to:

- Artificial intelligence (AI), machine learning, and natural language processing adoption.
- Robotic process automation (RPA).
- Cybersecurity and data privacy focus.

---

15. "Gartner Says 89% of Board Directors Say Digital Is Embedded in All Business Growth Strategies," press release, Gartner, Oct. 29, 2022, https://www.gartner.com/en/newsroom/press-releases/2022-10-19-gartner-says-89-percent-of-board-directors-say-digital-is-embedded-in-all-business-growth-strategies.

16. Chintan Shah, "Businesses Need to Watch these Digital Transformation Trends in 2023," Forbes, Jan. 27, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/01/27/businesses-need-to-watch-these-digital-transformation-trends-in-2023/?sh=7147b04a185d.

- Cloud migration.
- Data analytics.
- 5G adoption and digital optimization.
- Blockchain.
- Virtual business collaboration.
- Consumer data platforms.

Digital transformation's effect on GRC

Clearly, with so many connotations and applications, digital transformation has had a profound effect on GRC functions, and in many cases, organizations have struggled to maintain adequate levels of GRC coverage as changes in the technology landscape continue apace. A recent survey from Risk.net in collaboration with IBM of GRC professionals in the financial services sector revealed some alarming trends, including:

- 62% believe their digital transformation has exposed gaps in existing GRC processes, and nearly half of respondents (45%) think their organizations are now "playing catch up." Only 37% said they had invested time and resources toward their digital transformation before the shift.
- 77% believe their firms' risks have increased as they have become more reliant on digital channels.[17]

Additionally, in the same study, when asked what risks assumed greater prominence in their organization as a result of digital transformation trends, 56% identified information/data security, 48% said cybersecurity breaches, 32% said third-party/supply chain risk, and 31% said compliance risk.

To remain effective, GRC functions have had to modernize by taking definitive steps to embrace digital transformation or risk subjecting their organizations to significant risk. Such steps include:

- Allocating or recruiting new resources.
- Adopting some form of hybrid cloud data storage model for enhanced data analytics uses.
- Upgrading current GRC tools and capabilities.
- Deploying advanced technology, including AI-related tools and automation systems.

While some of these actions may seem somewhat obvious, the speed at which the current risk landscape is evolving makes them anything but. For example, historically, organizations relied on conformance to particular guidance or a framework of standards, certifications, and/or regulations to establish a foundation of proven controls and processes that set a GRC function up for success.

Today, however, such an approach can become complex quickly. This can be due to:

- The swift development of new or updated frameworks that require rapid conformance. Examples include the rapid creation of a variety of proposed regulatory initiatives in the EU related to digital strategy, including the Data Conformance Act, Digital Markets Act, Digital Services Act, Data Act, and AI Act, all of which anticipate approval by the end of 2023; or
- A lack of clarity or guidance from current frameworks, which leaves organizations — at least for a time — to fend for themselves.

[17] "Digital Transformation and the Future of GRC," Risk.net, IBM, Feb. 2022, https://www.ibm.com/downloads/cas/WWQXRPLG.

"With systems such as ChatGPT and Bing Chat coming out and CoPilot currently preparing for release, many organizations are needing to act quickly because employees are already using some of these technologies to complete tasks," said Sarah Kuhn, a noted internal audit leader with more than two decades of experience and service in the profession. "There are some organizations that will block them entirely, while others with teams more equipped to understand the technologies will create more detailed guidelines in-house on how and when it should be used."

Such teams tasked with developing strategies to create such guidelines will vary in makeup based on the organization, but they could include parties such as the chief digital and information officer, IT and risk management teams, legal, and finance groups. Once created, however, strategies to communicate and enforce the guidelines are equally critical. "Companies can operate on an honor system to some extent," said Kuhn, "but more formal measures to communicate evolving guidelines are needed, as well. For example, when an employee types in a certain address, there is a program that can be implemented that will have a banner pop up in their browser reminding them of the company guidelines."

To accomplish such a feat so seamlessly, Kuhn noted an agile, adaptable GRC function would need to be in place before emerging technologies such as ChatGPT entered the organization's risk landscape. Not every organization is going to have the blessing of such foresight, whether it is due to restricted resources, limited or poor-quality available data, prioritization of other issues, or simple negligence. Regardless of the reasons why, internal audit needs to be prepared to take the initiative to rapidly get GRC functions in a suitable position to succeed in this new era.

Internal Audit in the GRC Discussion

Improving GRC in the context of digital transformation

Keeping a seat at the table

Internal audit can support effective GRC in several key ways, especially in organizations that are considered behind on their goals of updating GRC functions.

First, few changes worth pursuing can be accomplished without a degree of investment. Such investments, however, can be difficult without buy-in from every level — from the top of the organization to each individual stakeholder in the GRC function. If there is no buy-in regarding digital transformation, there is a good chance its benefits are not being communicated properly. In this regard, internal audit is in a unique position to relay such information by simply maintaining a seat at the table.

"From our seat at the table, we can ensure through each emerging trend that management and the board are making informed decisions," said Kuhn.

Indeed, a seat at the table should always be critical for an internal auditor to perform their duties in accordance with their mandate. Through regular and informed communication with stakeholders, internal audit plays an invaluable role in promoting a strong organizational culture around risk assurance and compliance. When internal audit communication channels are leveraged to their full potential, GRC should never be far from top of mind.

The risk of GRC tool proliferation

Not all controls available to implement will be conducive to a successful GRC-focused culture. For example, with the digitalization of organizational processes, there are now many data analytics tools available that feature GRC modules as add-ons. Internal audit could find itself significantly hindered in communicating a comprehensive view of GRC to stakeholders if individual GRC functions all commit to the use of separate tools to assist them.

"I love data analytics tools and the 100% testing abilities they provide, but now there are so many other tools that add GRC to them as a value offering," says Audra Nariunaite, director of compliance at automated employment platform provider Oyster. "One tool I was recently looking at aggregates other SaaS tools to highlight which contracts are close to renewal and potential savings on taxes, but it also provides a version of a risk dashboard based on the information that SaaS tools process. If the intent of purchasing such a tool was for something different than GRC, I wouldn't even know about it."

"Suddenly, I could be in a situation where I would have a dozen random SaaS tools with components, all of them representing a high-level risk because vendors are processing our private information," Nariunaite continued. "Currently, there are over 100 SaaS tools in our ecosystem. Even if a small percentage of those tools offer a version of GRC for very specific processes, it becomes hard to manage. It creates individual pockets where people think they are doing risk assessments, but they are not doing them in a manner that's integrated in a holistic and reportable way."

To counter such a risk, one strategy is for GRC stakeholders to assign individual process owners to streamline the GRC approach and create a clear communication trail for internal audit. "Everyone wants to do the right thing," said Nariunaite. "There's a push for

managing overall risk now, and that is great. However, there need to be discussions about division of duties, and how they should occur to align priorities and scopes."

Kuhn expressed a similar sentiment by stressing the balance organizations should have between shared responsibility and top-down control. "Internal audit should try to let stakeholders drive GRC objectives and processes as much as possible, and then approach it from a context of promoting collaboration and transparency. Internal audit must be a part of that conversation, so we can be there to raise a red flag when we see something. Most people understand risk and control as it relates to their own roles. They don't really need us to interfere, but we need to understand the broader objectives and where responsibilities lie to perform adequate oversight."

Strategies to lead and promote discussion

Where possible, internal audit should lead by example by projecting and promoting the benefits of digital transformation through the effectiveness of its function. While some aspects of digital transformation within internal audit obviously require significant budgetary leeway, other aspects, such as basic automation, can be done through programs such as Excel, Power BI, and other Microsoft productivity tools likely already in-house, or at least purchasable at minimal cost.

Leading by example applies to the sharing of knowledge as well, including highlighting where critical competencies are lacking GRC functions. Both within the internal audit function and in other departments, internal audit can play a constructive role in highlighting gaps in workforce knowledge, training, or experience related to working with emerging technologies, while also promoting appropriate corrective measures. Such measures could include communal training at conferences, hiring external parties for training and upskilling, or simply incorporating skills-based training into job roles through free or reasonably priced online resources.

In some cases, organizations can work to promote upskilling in-house through interactions and collaborations with other departments. "One strategy I have seen is building a website where everybody in the organization can input their own innovation ideas, and then they can vote or comment on what they would like to see in the company," said Kuhn. "That would be a way to share knowledge and ideas in a controlled manner, so everyone isn't just going out and doing a thousand different things to build competencies."

Such discussion does not always have to be formal; even something as simple as a communal chat can produce a similar result. "In our organization, there are multiple Slack channels anyone can participate in," said Nariunaite. "Lately, for example, I've been hanging out in the engineering humor channel. They understand that I am the head of compliance, but they treat me as a partner. I love that we all can have informal connections with teams that are actually at the forefront of the digital transformation movement."

To be a contributing part of the discussion, however, there should be an added impetus on internal audit to become knowledgeable about these technologies.

Indeed, the acquisition of such knowledge can be a valuable opportunity for internal audit to add to the organizational value it provides. "I don't think we can meaningfully be involved in discussion with stakeholders when we ask to meet with them about, say, AI or data analytics, if we do not have a significant degree of knowledge in our own right," said Nariunaite. "So many aspects of digital transformation in GRC are still up for grabs regarding who is going to take ownership of them. Why not internal audit? We are curious; we have an open mind; and we are always learning alongside our clients so we can have a place in discussions. What if we were the ones that provided consultation for something like AI implementation in compliance?"

Conclusion

Be an active part of the internal audit community

There is no going back from a digital transformation, and the choices for an organization are simple: embrace or be left behind. Such a sentiment indeed flows through every element of the organization, from C-suite and boardroom down to GRC, operations, and internal audit.

Additionally, especially in an increasingly interconnected, globalized world, it should flow across industries and geographical boundaries. This means not just performing tasks within the boundaries of an organization, but also going beyond to be an active participant in global audit discussions. Participating in local IIA chapters can be a great place to forge such connections, as can regular attendance at IIA webinars and conferences.

"The best internal audit learning you can have is hearing first-hand the experiences of other functions," said Nariunaite. "I learn so much just 'nerding' out on current audit topics and tech trends with other professionals on Twitter. The profession has changed so much from when I started; it's so important to maintain those industry connections and keep a pulse of how others are successfully meeting the challenges you face."

Though technology has advanced so much — and will continue to advance — there is a degree of comfort in knowing that when it comes to learning and growing in a professional role, there is still no substitute for genuine human connection. In the face of unrelenting change, that will be important to remember.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 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

June 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