GLOBAL KNOWLEDGE BRIEF

The ESG Risk Landscape

Part 2 – Implementation, reporting, and internal audit's role

The Institute of Internal Auditors

Contents

About the Experts

Deon Annandale, CA

Deon Annandale is the CAE and general manager for risk management and internal audit of Remgro Limited, a diversified investment holding company. In this capacity, he also serves as CAE for various investee companies in the Remgro Group, which involves independent engagements and mandates from the boards of those companies. Previously, Annandale was head of internal audit at Dorbyl Limited, and regional audit manager for BHP Billiton.

Luis de la Fuente, CIA, CRMA

Luis de la Fuente serves as head of internal audit for sustainability and ESG risks at BBVA, reporting to the chief audit executive of BBVA Group, a Spanish multinational financial services company. He has more than 20 years of experience in internal audit and has served as head of internal audit for BBVA Spain, BBVA USA, and BBVA Corporate & Investment Banking.

Douglas Hileman, FSA, CRMA, CPEA, P.E.

Douglas Hileman has 40 years of experience in compliance, operations, auditing, and nonfinancial reporting supporting clients nationwide. He has experience with multiple lines through work with operations and corporate compliance, EHS auditing, internal audit, and external assurance (supporting financial audits and conducting conflict minerals independent private sector audits), and has been involved in professional organizations dedicated to EHS auditing since the 1980s.

Charlotta Löfstrand Hjelm, CIA, QIAL

Charlotta Löfstrand Hjelm has more than 20 years of internal audit experience as CAE in both the public and private sectors. She is currently chief internal auditor at Länsförsäkringar AB, a Swedish insurance and banking company. She previously was senior financial officer (CFO) and director with AFA Insurance. She is also a board member at the Swedish Audit Academy.

Edward Olson, CIA, CFE, CPA, CA

Edward Olson is leader for environmental, social, and governance with MNP, a Canadian accounting, tax, and consulting firm. He also provides risk management, internal audit, corporate governance, and regulatory compliance services to his private and public sector clients. Prior to joining MNP, Olson led the advisory services practice for a different Canadian public accounting firm. He also was the chief audit executive leading internal audit and risk management at a Canadian electric power and gas distribution/retail company, general manager for an alternative energy company, and was a partner in a firm where he acted as an outsourced CAE for clients in the financial services industry.

Introduction

There is little argument that Environmental, Social and Governance (ESG) risk has become a permanent part of the modern risk lexicon. The need for independent assurance on the design and efficacy of ESG-related processes and controls will soon be essential to the work of internal audit. Just as evolving risk has expanded the profession's scope of services beyond financial reporting to include compliance, operational, and cyber risk, so too will it be for ESG-related risk. As such, internal auditors must be prepared to act confidently and authoritatively in support of their organizations' ESG efforts, particularly in instances where such efforts are new to the organization.

The challenge for many practitioners will be how to deliver high-quality assurance and advisory services that add value in a risk area that is quickly evolving on several fronts, including:

- Understanding the scope of ESG risks.
- Implementing models and frameworks for related controls and processes.
- Overcoming uncertainty about reporting and reporting standards.
- Managing ESG risk holistically across the organization.

Strong organizational governance over all aspects of ESG risk, from data governance to reporting, should drive internal audit's work in this area. This requires alignment in roles and responsibilities among the board, executive management, and internal audit as outlined in The IIA Three Lines Model[1]. The following provides an overview of internal audit's responsibilities relating to providing objective assurance, insight, and advice on effective ESG practices, risk management, and reporting. It should be considered in conjunction with parts 1 and 3 of *The ESG Landscape* series published by The Institute of Internal Auditors.

1. The Institute of Internal Auditors, "The IIA's Three Lines Model," *The Institute of Internal Auditors*, https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated.pdf.

Implementing ESG

Evaluate current status as a starting point

Several models are available for designing, implementing, and evaluating ESG programs. Even a cursory internet search will turn up models from the prominent audit firms, accounting and professional service firms, IT/software vendors, professional organizations, and academic organizations.

Each emphasizes different points and approaches, but the underlying principles and concepts should look familiar to internal audit practitioners and their stakeholders. For example, COSO's Enterprise Risk Management Framework and its Internal Control – Integrated Framework are agnostic with regard to topic. They are adaptable to risk management and external (ESG/sustainability) reporting, respectively. ISO management systems standards and others follow the familiar cycle of plan, do, check, and act.

As a first step toward implementation, organizations need to take stock of what is already in place, said Doug Hileman, a consultant in compliance, operations, auditing, and non-financial reporting. Many ESG topics are well established and are regulated by a variety of agencies globally. For example, in the United States, the Environmental Protection Agency, Occupational Safety and Health Administration, Department of Labor, Department of Commerce, and other agencies have established regulatory and reporting regimes. However, reporting in such areas has been done primarily to fulfill regulatory requirements.

Many companies use ISO management systems to formalize processes in ESG topical areas, including environmental, safety, and energy management. Some companies have extended coverage of management systems to include some content included in ESG reporting. Still, these management systems may not rise to "investment grade" internal controls expected by capital markets.

A company may find that various components of ESG are in different stages of maturity, having originated in different parts of the organization. Hileman suggests cross-functional teams are an excellent way for departments, including HR, Investor Relations, and Operations, to build common understanding of issues, risks, stakeholder expectations, systems, and controls.

COSO's internal control framework has relevance for ESG reporting, Hileman said. In early days of the U.S. Sarbanes-Oxley Act of 2002, companies found they had strong programs in some areas, but room for improvement in others. It is the same situation now for ESG reporting, but it may be more difficult this time for several reasons, he said. First, ESG reporting is not as mature as financial reporting was when Sarbanes-Oxley was passed. Second, ESG covers many topics, with homes in different parts of the organization, which historically have not communicated with each other about topics within their

Remgro, BBVA: Putting ESG assurance to work

Enterprise-wide risk management at Remgro Limited, a South African diversified investment holding company, is based on COSO's ERM framework, said Deon Annandale, CAE and general manager for risk management and internal audit. The internal controls process and environment also are aligned and assessed based on the COSO Internal Control– Integrated Framework. These frameworks form the foundation for Remgro's approach to ESG risk management and reporting, he said.

As a financial services company, BBVA is heavily regulated and supervised, said Luis de la Fuente, the Madrid-based bank's head of internal audit for sustainability and ESG risks. Rather than focusing only on reporting, internal audit at BBVA has a strategic goal in making sure the company manages its risks properly. BBVA has embraced sustainability as a core part of its strategy, he said. Internal audit accompanies the business units through their maturation process. This automatically helps align interests between business lines and internal audit, because by taking the lead in sustainability, the bank

own specialty. In addition, the need is new for reasonably consistent internal systems and controls that are sufficiently robust to support external reporting to capital markets.

Ensuring Completeness and Accuracy

Robust management systems are important factor

As with any risk area that involves public reporting, internal audit should play a critical role in ensuring data completeness and accuracy. The likely assurance requirements that will be part of the European Union's Corporate Sustainability Reporting Directive, along with hints of the same from the recently created Internal Sustainability Standards Board (ISSB), underscore the expectations for complete and accurate ESG data. Still, challenges exist in ensuring the completeness and accuracy of data and information. This can be expected, Hileman said, given where this data originates (HR, Environmental, Procurement, Sales, etc.) and how their systems and controls developed independently.

Additional challenges stem from parameters of some ESG topics extending beyond the boundaries of the organization and into diverse areas that stakeholders expect them to influence. Increasingly, shareholder expect diversity and inclusion requirements to extend to contractors. As another example, the Greenhouse Gas Protocol's Scope 3 emissions include supply chain, transportation, product use, and disposal, which are often the largest contributors to greenhouse gas emissions yet operate outside the purview of many organizations.

The risks associated with meeting public expectations on managing third-party ESG matters can quickly meet the well-established bar of "likelihood and impact." One high-profile retailer suffered reputational damage when it became known that the landlord's parking system used an app that tracked customers' browser usage. The retailer's explanation that it was not in control of the app fell flat. This lack of boundaries is in contrast to the rigid boundaries that exist for financial reporting, which have been established for years and are subject to regulation and accounting practices.

This kind of situation is all the more reason for companies to focus on ensuring — or building — robust management systems with a strong control environment that require the same rigor as controls over financial reporting, said Edward Olsen, an ESG leader at Canadian accounting, tax, and consulting firm MNP. The criteria for some controls are well developed, such as for Scope 1 and Scope 2 greenhouse gas emissions. Internal audit has relevant experience and is well positioned to help companies in these areas, he said.

At Remgro, the board established, through its audit and risk committees, a combined assurance process designed to ensure all relevant and reportable non-financial information is assessed for completeness, accuracy, validity, and relevance, Annandale said. External consultants validate data used in submissions on environmental impact to the CDP, for example. The processes at both Remgro and its subsidiary companies include comprehensive control processes, technology, and reporting systems; validating reports that have been generated; and control assessments by internal audit and consultants. Reports generated at individual company levels and reported up to Remgro are reviewed by the responsible C-suite-level officers, who sign off on the controls, environment, and processes used to generate the reports.

Risks Associated with ESG Reporting

Lack of strong controls can cause problems

The risks associated with ESG reporting mirror those of financial reporting, Hileman said. The content of the reporting may be incomplete, inaccurate, not supported, or not verified. Alternatively, the content may be altered by unauthorized parties, perhaps intentionally for some type of gain, such as a reducing capital costs for green investment instruments or gaining advantage in a government contract.

Annandale said the primary risk from ESG reporting is to corporate reputation. There is always the risk that the focus on frameworks and tick-box approaches could overshadow and become misaligned with the board's strategic intent. The intent of ESG reporting is to ensure that Remgro and its companies make responsible investment decision, Annandale said. Integrity and stakeholder trust is fundamental to the whole process, he added.

Other risks include:

- Compromise of the credibility and usefulness of the reporting process if inappropriate indicators and/or frameworks are used in aggregating and reporting information.
- Invalid and misleading information stemming from inadequately designed controls and systems.
- Compromises to credibility because of overly optimistic assumptions in setting targets.
- Reporting beyond the minimum standards and raising stakeholder expectations that may not be met in practice.

Regarding ESG, Annandale said disclosures need to avoid the risk of non-compliance, and at a minimum need to be compliant with legal requirements. The Johannesburg Stock Exchange is moving toward mandatory disclosure, having launched ESG disclosure guidance in December 2021.

Other risks include:

- General misalignment risk, where ESG reporting is inconsistent with other financial disclosures or corporate communications.
- ESG is seen as a 'box-ticking' exercise. This is a strategic risk because the underlying goal of the ESG policy is to drive a transition to sustainability. Meeting this goal implies business innovation and perhaps changes to core activities, strategies, and even business models.
- ESG is seen as marginal rather than central to a company's activities.

De la Fuente said the main risks are errors, both intentional and unintentional. He noted that controls in ESG reporting and non-financial reporting are not as robust as those for financial reporting, have a shorter history, and generally are not being reviewed by an external firm. Internal audit can provide value by reviewing the controls, he said.

However, both banks and other businesses face a number of risks if they are not successful in understanding and managing ESG issues, de la Fuente said. They include:

- Impact on business model. Investors likely will push publicly listed companies to adopt sustainability practices. Companies not attentive to ESG issues could lose their competitive position.
- Limitations on sources of capital, or higher costs for capital.

- Regulatory risks.
- Demands for corporate responsibility from employees as well as customers.
- Harm to a company's ability to attract customers and employees, who expect companies to imbed ESG factors into their business.
- Social and geopolitical implications, such as localized social or civil unrest.

Roles of Internal Audit

Unique perspective allows a systematic approach

Internal audit has clear roles in providing assurance and advisory ESG services, and its experience and place in the organizational structure suggests even more roles that can add value to the organization. Internal audit's unique position within the organization allows it to help guide it to a systematic approach to ESG, embrace the coming changes, and put sustainability goals and theories into practice.

Assurance

Internal audit at BBVA tries to provide both assurance and advisory services, especially on governance, de la Fuente said. Factors under consideration include how the company sets its strategy, how sustainability is considered in the business model, whether roles and responsibilities are clear, and whether good reporting to the board has been established.

Internal audit is paying attention to these areas now because eventually, with a little more maturity, it will be able to provide assurance to products and processes, he said. Governance, environmental issues, and reporting disclosures are the bank's main priorities right now, which reflect European priorities, de la Fuente said.

Although ESG systems and controls are not "assurance ready" for many aspects of assurance, the demand for external assurance from capital markets is undeniable. Internal audit should pre-emptively gear up to fulfill a role for ESG reporting to capital markets, just as it did for internal controls over financial reporting in the wake of Sarbanes-Oxley. Otherwise, companies will be faced with external auditors looking at ESG systems and controls before they are mature and without internal audit having a first look.

De la Fuente listed several ideas on how internal audit can begin offering advisory services if a company is just getting started in ESG. First, do not look at areas where regulations are in place or where policies and procedures have been established for some time, because sufficient criteria already exist to perform assurance over those areas. Instead, initiate management discussions in areas that are less defined and not ready for assurance, such as those involving guidelines or expectations from regulators, he said. Non-financial reporting, voluntary frameworks and supervisory guidelines (not rules) are great opportunities to help improve governance and risk management through advisory engagements. "We test the waters on the topic. We focus on issues that are emerging," de la Fuente said. However, management approves all engagements.

Annandale said internal audit is ideally placed to be a major assurance provider in the ESG and non-financial reporting process. Internal audit has deep corporate knowledge and per its mandate already assesses culture, ethics, governance frameworks and processes, internal reporting, combined assurance, internal control, control environment, and compliance. What's more, it has knowledge of fraud and related risk.

Internal audit leaders and practitioners should recognize that ESG-related assurance engagements will come to them, Hileman said. Once external assurance is required by a law, regulation, or standard, the board can be expected to turn to internal audit for assurance ahead of work by the external auditors. "This is why IA should discuss this with the board and management, and develop the pathway to assurance," he said.

Advisory

Internal audit should advise on the risk landscape of ESG as it pertains to reporting to capital markets, competitive advantages and disadvantages, compliance (as broadly defined), operational efficiency and effectiveness, and reputational risk. This role lends itself to advisory efforts as issues evolve, de la Fuente said. Internal audit can play a useful role from start to finish by identifying the issues, having discussions with management and the board, planning, getting the pulse of organization's readiness and opportunities, and providing insights to reduce risks and leverage opportunities. This goes to the heart of the company's ESG strategy and success – or failure.

Advisory engagements can help the organization understand risk, focus on the right issues, and chart their path forward. Internal audit should use their familiar planning skill sets to identify topics, socialize them with management and the board, and build reasonable consensus for advisory engagements. Once these are done audit procedures will look much like any other audit.

In addition, there are advisory work opportunities including, benchmarking, strategy and appetite considerations, framework selection considerations, KPI development, resource requirement assessment, reporting considerations, and assessing the overall benefits of sound ESG practices.

Internal audit also can embrace other roles that can add value to an organization's ESG journey without compromising independence or objectivity.

- **Advocacy:** ESG topics traditionally are widely dispersed in an organization, and there may be no single point of contact for external ESG reporting and disclosures. When it does have a home, it may be a function without authority, resources, or skills to fulfill this important activity. Internal audit can advocate for the company to approach ESG just as it would approach any other risk: seriously. Internal audit also should advocate for its own role in the pathway to assurance.
- **Convener:** If internal audit has not had discussions with the board on ESG, it should initiate these. Internal audit should be involved in all such discussions. Internal audit can suggest or evaluate cross-functional teams, convening functions in the organization that should be involved in ESG strategy, reporting, disclosures, and risk management consistent with business strategy and goals.
- **Capacity building:** Internal audit should build its own capacity. This can be internally, with co-sourcing, or using external resources – including ESG specialists. Internal audit may identify insufficient capacity to manage ESG risks and opportunities at the organization; these insights can serve as advocacy to justify capacity in first or second lines of governance.

The only way to advance is by asking for information, analyzing the data, and initiating discussions with management. Management, "wants to do a lot of things; they don't have the time, and they don't know where to start," de la Fuente said. This is where internal audit has a crucial role to play, he said.

Skill Sets for Internal Auditors

Knowledge of financial auditing transfers to ESG

Auditors with a background in financial auditing have the skills to do non-financial auditing, although they may need training on some issues, such as regulations applicable to their particular country and knowledge on ESG analysis, de la Fuente said. The CFA Institute's certificate in ESG Investing as well as the ESG Analyst certification offered by the European Federation of Financial Analyst Societies (EFFAS) can serve as an entry point into ESG auditing for auditors who already have the background in financial reporting. These certificates provides a financially viable opportunity to add ESG knowledge and skills for smaller audit functions, which typically cannot afford to hire engineers or engage consultants, de la Fuente said.

Internal auditors can build off the skills they use elsewhere, said Hileman — curiosity, professional skepticism, courage, persistence, knowledge of the organization, familiarity with the subject matter (or the assistance of someone who is familiar), as well as communications skills. It also would be helpful for internal auditors to have some background on the history and rapid evolution of ESG reporting – the expectations, risks, and opportunities. Internal audit also should develop a comfort level with advisory engagements, he said. While the front end of such engagements –identifying topics, having discussions, developing a consensus, planning – look different, the engagements themselves should look and feel familiar.

Annandale said that in addition to the skills already required from proficient internal auditors, consideration should be given to:

- Effective, influential, and inspirational communication.
- Governance best practice.
- Technology driven assurance processes in non-financial data.
- Trusted advisor attributes.

Internal auditors have the time to train and to think about such areas as sustainability issues. In addition, internal audit can help management be more aligned with its strategy and to be more effective, de la Fuente said. For example, if BBVA is successful in deploying a sustainability strategy and in helping its customers become more sustainable, it in turn will become more effective at mitigating ESG risks, he said.

In addition, ESG technical specialists can add value to internal audit and to organizations themselves. Annandale noted these skills complement the skills of auditors, while de la Fuente said technical specialists would be especially useful for small audit shops, which may not be able to afford to hire in-house specialists. Added Hileman: "ESG is not a monolith. Climate change, work force equity, forced labor in a supply chain, habitat preservation, and privacy are very different. Some assistance can be useful in establishing priorities and programs at a high level."

Closing Perspectives and Tips

Deon Annandale

At Remgro, governance authority for ESG is vested in the board of directors. The board in turn established a strategic ESG committee that reports to the board, along with an ESG operational committee that reports to Remgro's board. The board's remuneration committee links KPIs for the ESG process to the achievement of various performance indicators.

Integrated thinking (about both financial and non-financial concurrently) offers another window on more effective risk management and value creation. Remgro applies COSO"s ERM to ESG risks. This allows it to integrate ESG principles and practices into the company's broader ERM framework. In addition, Remgro uses PESTLE[2] (Political, Economic, Social, Technological, Legal, and Environmental) analysis as a framework to assess emerging risk and opportunities.

Luis de la Fuente

Internal audit should first help organizations understand how ESG applies to them, not just for compliance and risk management. Reporting is the first thing audit functions should be incorporating into the program for ESG.

De la Fuente underscored the importance of data, as well as the need to be proactive. From an auditing perspective, when addressing social related issues, "I think it is important to sit at the table with management with abundant data." Using data supports internal audit's case rather than simply discussing generalities. "I think it's important that you do your math and crunch the data and have some ideas to throw to management."

BBVA's internal auditors adopted one simple convention that has improved engagement with their internal stakeholders: Internal audit does not assign a rating on an advisory engagement. Instead, they issue recommendations, do a follow-up, and wait at least 12 months before considering a "rated audit." Internal audit understands that, as an emerging issue, many elements of risk management and internal controls likely will be lacking, and a traditional rated audit would consider those as gaps or deficiencies, resulting in a "bad grade." This, in turn, can influence mangers' compensation, reputation, and chances for promotions, which is hardly the way to encourage auditees to provide full, truthful information. These advisory engagements are an opportunity for insights and help, de la Fuente said.

De la Fuente mentioned the forward-looking thrust of ESG programs and reporting. Internal audit can play a role in value creation. Because banks play a central role in the economy, this value — financial and otherwise — extends beyond the bank into communities and the overall economy for a more sustainable world.

Doug Hileman

Hileman noted that the term "greenwash" is common, and said internal auditors should go further and consider ESG fraud, which may not look like the usual misappropriation of assets. Data analytics (Benford's law, etc.) may not be useful in the

2. Oxford College of Marketing, "What is a PESTEL Analysis?", *Oxford College of Marketing*, https://blog.oxfordcollegeofmarketing.com/2016/06/30/pestel-analysis/.

traditional sense, but it will evolve. Insist on a fraud brainstorming session for any type of ESG effort – planning, advisory, assurance, or advocacy, and become a champion for prevention and detection of ESG fraud.

Hileman also noted that many organizations have second-line audit functions such as IT, environmental, quality, or safety with staff and systems IT platforms that can be adapted to the current demand for ESG information. However, many of these second-line audit programs remain mired in their original purpose. They typically have not had a quality assurance review, and many focus exclusively on regulatory compliance, not on other risks (including external ESG reporting to capital markets). Internal audit should take the initiative to improve and leverage these resources, being careful to monitor and recognize the appropriate separation of second- and third-line responsibilities, as outlined in The IIA's Three Lines Model.[3]

Finally, Hileman noted that ISO management systems standards initially focused on "training," but have changed to "competence" in recent revisions — a subtle, but important difference. The high profile of ESG has led to an influx of ESG professionals with areas of focus as broad as ESG itself, from green buildings to renewable energy or sustainable textiles. While many of these ESG professionals are competent, some entered the field driven by passion and offer less value to organizations looking to mitigate risk and create value. Be discerning in resourcing decisions and invest in conferences, useful certifications, continuing education, and coaching to ensure that employees can contribute to the success of ESG audits and programs.

Edward Olson

Olson emphasized the need for tailoring ESG implementation to each organization. Risks, opportunities, and requirements vary by industry, geographic location, regulatory environment, policy environment, and a host of other drivers and influences. Other companies' programs can provide useful precedents, and vendors offer "solutions" – but all will require customization.

Olson also notes a different kind of accountability. ESG disclosures include targets, and the reporting frameworks require the inclusion of prior years' performance on these parameters. Analysts and capital markets will follow these and will hold management and boards accountable for their progress (or lack thereof). Failure to achieve targets or simply making boilerplate disclosures on how the company attempted to achieve the targets can have ripple effects from financial institutions, customers, or other stakeholders.

Finally, Olson put a different twist on a classic step in risk management. One option to address risk is always to "do nothing" and accept the risk posed by the current condition. The degree of attention on ESG, the pace of change, and the very public nature of ESG reporting and disclosures all point in one direction: Do something.

3. The Institute of Internal Auditors, "The Three Lines Model",

About The IIA

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 210,000 members and has awarded 180,000 Certified Internal Auditor (CIA) certifications worldwide. The IIA is recognized as the internal audit profession's leader in standards, certification, education, research, and technical guidance throughout the world. For more information, visit https://www.theiia.org.

Disclaimer

Copyright

February 2022

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