Internal Audit and ESG: Opportunity or Obligation?

Highlights of Presentation for IIA Brazil - November 8, 2021

By Douglas Hileman, FSA, CRMA

Douglas Hileman presented to IIA Brazil's conference on Environmental, Social and Governance (ESG) on November 2021. He offered perspectives from over four decades of relevant ESG experience. Here are some highlights. The slide deck is available (in English); contact doug@douglashileman.com. To be available in Portuguese, courtesy of Mr. Alexandre Rossin, at alexandre.rossin@mac.com.

ESG Reporting is creating tremendous "pull".

There are several reporting ESG standards and frameworks. The demands from capital markets have been in the news: SASB, Integrated Reporting Framework, TCFD, and IFRS. There is some alignment underway, notably with creation of Value Reporting Framework (combining SASB and the IIRC in 2021). In November 2021, IFRS announced creation of an International Sustainability Standards Board (ISSB), consolidating VRF with the Climate Disclosure Standards Board. This consolidation is intended to produce consistent, comparable useful information to the capital markets.

There are other ESG reporting standards and frameworks aimed at capital markets – for example, for green bonds, green investment funds, and other ESG specific purposes. These frameworks go well beyond the larger frameworks. They are mostly principle-based, and are still evolving in maturity, reliability, and usefulness.

There are other public ESG reporting frameworks – notably GRI and CDP. Both include many reporting topics, and both ESG reports are intended to be public.

Organizations are obliged to do even more ESG reporting to a range of business partners. Each reporting obligation has its own scope, parameters, requirements – and risks.

Management and Compliance functions should look to ESG reporting frameworks as the starting point for evaluating ESG risks and opportunities. ESG reporting frameworks for capital markets are in the spotlight, and are the logical place to start. However, there are other ESG reporting frameworks (even for stakeholders in the capital markets) that also offer risks, opportunities, and clues for emerging issues.

ESG and Compliance: It is Getting More Complicated

Regulatory compliance requirements are growing. Topics, scope, applicability are changing. Compliance requirements can include publicly available reporting. Here are three examples.

Conflict Minerals: This was the first ESG-specific rule by the SEC. The rule requires due diligence in the supply chain for tantalum, tungsten, gold ("3TG") in products. The rule a standalone submittal to the Securities and Exchange Commission – not embedded in other financial filings. The SEC rule provides parameters for a voluntary independent assurance audit. Industry had to develop a new data exchange standard, so companies could provide required information without disclosing intellectual property. SEC has jurisdiction over companies that are publicly traded in the U.S. The SEC cannot pursue enforcement against other companies. However, all companies in the 3TG supply chain were affected. They had to comply with customer requirements or lose sales.

UK's Modern Slavery Act applies to companies with >36 million British pounds annual revenues in UK. It applies to company operations worldwide. Companies must provide training on human trafficking, take steps to mitigate risks in supply chain, and publish reports. In 2019, UK began moving from "suggested" to "required" topics in these reports. In 2021, UK launched a public registry, where statements and disclosures can be accessed. Manufacturers, retailers and professional service firms with >36 million pounds in revenues from UK were surprised to learn they were now required to implement due diligence efforts worldwide, and publish reports on their efforts in the UK.

Brazil's Central Bank has announced that climate change related financial risks will be included in bank stress testing, beginning in July 2022. Brazil follows the lead of central banks in several other countries. Climate change related risks are not just environmental – they are also financial. They could be significant enough to pose risk to financial institutions. This will become a compliance requirement for banks. But banks will need to evaluate this somehow – likely by evaluating their portfolios. If you are in energy, retail, mining, real estate or any sector … if you depend upon a bank for financing, this will become a risk for you. If financing agreements include provisions that require disclosures of climate change related financial risks – now it's a compliance requirement.

Recognize how compliance requirements have grown and changed. Today's risk is tomorrow's compliance requirement. Internal Audit should incorporate the full spectrum of ESG requirement obligations in annual risk assessments, developing annual audit plans, and in doing audits.

ESG Systems and controls aren't ready for external assurance.

There are demands for external assurance of ESG reporting and disclosures.

However, systems and controls for ESG topics are not mature enough to undergo assurance. There have been internal controls over financial reporting (ICFR) for decades. For ESG reporting – not so much.

ESG doesn't have a logical "home" in many companies. ESG consists of many topics – some old, some new. Roles and responsibilities for ESG lie in Human Resources, Operations, Environmental, Quality, Legal and many other departments. Some programs grew to meet regulatory compliance requirements. Others began for marketing purposes, or to coordinate internal efforts.

Management and Compliance functions should evaluate existing systems and controls in light of current requirements, risks and needs. Internal Audit should gear up to perform assurance over internal controls for non-financial (e.g., ESG) reporting. The first step would be to survey the landscape of ESG internal controls for ESG reporting – to capital markets and any other external ESG reporting (e.g., public, to customers, etc.). Such a survey may highlight significant risks to the company.

There are second line audit activities for many ESG topics: environmental; quality; safety; etc. These functions have not grown with the ESG risks, and may not be very helpful in mitigating current ESG risks. Second line audit functions have useful skills, but they do not have the charter or authority to expand their role.

ESG Fraud is a possibility – and will happen.

Fraud is any deceit for a gain at the expense of others. The Cressey fraud triangle consists of incentive, opportunity, and rationalization. Where all three exist, fraud can happen. ESG is no different from any other situation where people can be tempted to deceive others for some type of gain.

ESG offers incentive for inclusion in green investment funds, favorable impressions for customers or the public, awards or prestige. Weak or inconsistent controls provide the opportunity. There are many rationalizations ("it's not about money, exactly" or "Everybody does it".)

The Volkswagen diesel emissions event is probably the most well-known ESG fraud. It wasn't the first, and it won't be the last.

Management and Compliance functions should design systems and controls to prevent fraud. Internal Audit should include fraud detection steps in each annual risk assessment, risk assessment for each audit, and all audit procedures.

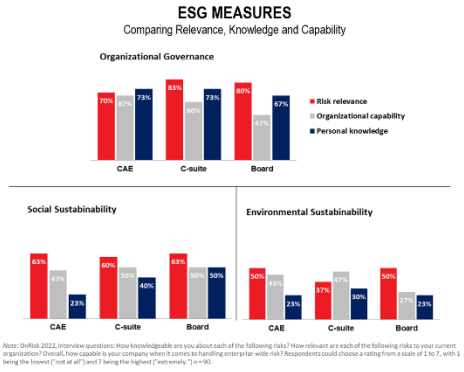
Internal Audit can – and should – play multiple roles for ESG.

Assurance: Internal Audit can perform assurance engagements. This is a core strength of Internal Audit. It works best when audit criteria are well-defined, and where the conditions to be examined are clear. Both are in a state of flux for ESG.

Advisory: Internal Audit can also perform advisory engagements. These can be useful when criteria or risks are dynamic, or when audit sponsors have specific needs. This is the current situation for ESG.

Advocacy: Internal Audit can also add value through advocacy roles. IA should be part of communications with the Board and Management. They are having conversations with external auditors and many other stakeholders; IA should be aware of these discussions, and provide their own distinctive perspective. IA should advocate for more resources to prepare for the expected demand to provide assurance over ESG reporting. IA can also advocate for second line assurance functions to revise their charter and activities, to mitigate current risks and add value to the organizations.

.



Internal Audit has a unique vantage point. IA sees the entire organization. IA is independent. It can use resources internal to the department or company, or it can procure external subject matter expertise. In short, Internal Audit has a powerful toolbox that can – and should – be used to help achieve and maintain compliance, address stakeholder needs, mitigate risks and seize opportunities arising from ESG.

Internal Audit Calls to Action

Internal Audit should step up to provide value to their organizations. In fact, the biggest risk to Internal Audit is being left behind. As my co-presenter said, "just do something!" Here are five calls to action.

1. Include ESG in annual risk assessment.
2. Take an active role in assuring internal controls over non-financial (ESG) reporting – especially for capital markets.
3. Use the flexibility and power of Advisory engagements.
4. Recognize that ESG fraud can occur, and include procedures in audits.
5. Develop capacity, and use the best resources to get the outcome you need.

About the Authors

Doug Hileman helps clients with ESG compliance, risk management, reporting and auditing. His experience extends to a range of ESG regulations. He has experience with ISO management systems frameworks, COSO internal controls and risk management, GRI, OECD, accounting rules, and SASB. He was the senior environmental management and environmental auditing specialist on the Volkswagen Monitor Team. He is active in the Institute of Internal Auditors, where he has presented on ESG issues for over a decade and has authored guidance documents available to over IIA 180,000 members worldwide. See www.douglashileman.com.

Alexandre Rossin is a special contributor to this document. Alexandre Rossin helps clients with ESG programs, including ESG evaluations and controls for green investment instruments, and environmental compliance and risk management. Mr. Rossin is native to Brazil. Rossin International LLC supports clients worldwide on ESG risk, compliance, reporting, and finance-related issues. Rossin International is based in U.S., supported by a network in Brazil and elsewhere. Douglas Hileman Consulting thanks Mr. Rossin for providing this summary in Portuguese. Mr. Rossin is at alexandre.rossin@mac.com.