How internal audit can integrate ESG into third-party risk management

Michelle Hurley
Senior Product Marketing Specialist
Wolters Kluwer TeamMate

Kevin Gould
Audit Committee Chair and
Internal Audit Consultant

Wolters Kluwer

Contents

Introduction	3
Characteristics of ESG issues	4
Key stages of third-party management	5
Integrating ESG into third-party risk management	6
How internal audit delivers value	7

About the authors

Michelle Hurley
Senior Product Marketing Specialist, Wolters Kluwer TeamMate

Michelle is a Senior Product Marketing Specialist for Wolters Kluwer TeamMate where she develops and drives engaging marketing, customer outreach and sales enablement programs. Michelle uses her experience working with audit departments to influence the product roadmap and gauge the value of TeamMate+ to help audit departments in overcoming the challenges facing their industry.

Kevin Gould
Audit Committee Chair and Internal Audit Consultant

Kevin is a Chartered Accountant with a strong background in internal audit and a recent focus on ESG. He has more than 25 years of experience as a consultant, adviser, and auditor. Kevin has a long-held interest in sustainability and a Masters in Sustainability & Environmental Management. He is now an independent consultant, as well as being a non-executive director and audit committee chair on several boards.

Introduction

When it comes to managing Environmental, Social, and Governance (ESG) risks, are you leading the charge or just getting started? Regulators, investors, stakeholders, and even the public expect more from companies beyond brand recognition and profits. And over the past few years, there's been a shift in how organizations view ESG practices. Once considered a "nice to have" and something to be considered down the road, ESG is now a strategic imperative.

However, working with third parties may potentially undermine your ESG risk management. As with any risk, internal audit teams must ensure that third-party vendors align with their ESG goals. It's important to also understand that your third parties (vendors and partners as well) may maintain their own network of third parties which, as a trickle-down effect, could negatively impact your organization.

Internal audit must consider and, ultimately, understand their organization's appetite for ESG risk, especially as it relates to third-party providers and suppliers. Organizations are likely to have different risk strategies for varying ESG areas. But as internal auditors, you need flexibility in how that is expressed. It may be part of a broader approach to risk assessment, whether explicitly defined or implicit in that approach. What's important is that it is clearly and consistently understood.

As with any risk, internal audit teams must ensure that third-party vendors align with their ESG goals.

Characteristics of ESG issues

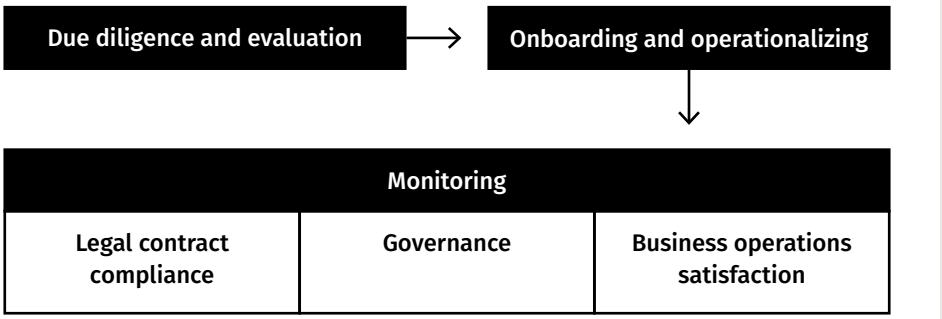
ESG factors are often used to evaluate a company's commitment to sustainable operations. The environmental factors in ESG offer insight into an organization's environmental impact, including its carbon footprint, climate change initiatives, waste management policies, natural resource conservation, pollution, or efforts to decrease deforestation. The social component of ESG looks at an organization's treatment of stakeholders (workforce, customers, providers and suppliers, government, regulators, or the local or global community) on issues such as diversity, equity and inclusion practices, wages and salaries, and sales practices. Finally, governance factors assess whether a company's internal processes ensure the organization and its employees act with professionalism and integrity.

Stakeholders are increasingly expecting long-term stewardship rather than a focus on short-term profits. Organizations are focusing on value creation through more sustainable business models to meet the demand. Most of the governance frameworks, whether optional or mandatory, reinforce this. This also includes considering impacts outside an organization. Many stakeholders expect an organization to take responsibility for any consequences that originate in third parties or even throughout the entire value chain, furthering the need to consistently be aware of your third-parties' ESG risks, initiatives, and strategies.

Key stages of third-party management

A third party is defined as any business entity that (often, but not always) has a written agreement with an organization to provide products or services to their customers or on behalf of the company. Working with third parties like software providers, general suppliers, delivery and cleaning services, call centers, consultants, or contractors can help businesses fill gaps in current capabilities, increase efficiency, and more. Yet, internal audit teams must also ensure that their organization accounts for any and all potential risks introduced by leveraging third parties. And although internal auditors can't utilize the same risk controls as if these activities were happening in-house, they should expect to see adequate controls and the necessary assurances aimed at reducing these risks.

As organizations build and maintain their third-party networks, here are the key stages for successfully managing these relationships:



Due diligence and evaluation

This is the first step in the search process, where an organization builds a business case or requests additional information to identify possible partners and areas of potential risk. The due diligence process and evaluation stage should be a defined and well documented process within an organization.

Onboarding and operationalizing

Once due diligence is complete, a vendor is selected, and contracts are signed, the next step is to get the relationship up and running. As soon as the third party is declared operational, the business owner is expected to manage the relationship.

Monitoring

Monitoring is a critical step in the third-party risk management process. Throughout the relationship, the business owner periodically evaluates whether the vendor's performance meets expectations. There may be performance metrics to measure success in terms of productivity, efficiency, or return on investment that have been established during the due diligence and onboarding process. The business owner should make note of any changes or updates to that vendor agreement and keep the organization informed of any potential risks.

Additional considerations during the Monitoring stage include:

Governance

This is straight forward but it's worth mentioning that it also includes IT risk and governance, especially as more organizations dive into cloud services. It's critical to ensure that data privacy rules and regulations are complied with, and that data is secure and protected.

Legal contract compliance

Ensure the contract is in writing and, more importantly, that mechanisms are in place to comply with the contract's essential terms. Legal, Procurement or the Business Unit may be responsible for the ongoing monitoring of all legal and contractual obligations for both the organization and the obligations of the third party.

Business operations satisfaction

Continue to measure the relationship against the risk requirements that have been established. This stage may require a large amount of record keeping and documentation. As such, the business should periodically assess the third-party relationship and determine the level of satisfaction. Measurement back to the original drivers should be completed and documented to ensure the organization is receiving the level of service and/or quality of product that was originally agreed upon.

The challenge here is that third-party management can be informal and typically adhoc, and internal audit have often reported a lack of communication between the internal stakeholders which provide a broader based monitoring process.

Integrating ESG into third-party risk management

With the increasing importance of ESG to all organizations, organizations will likely face amplified risk exposure relating to ESG in their third-party relationships. One of the most common ESG risks, as it relates to third parties, is reputational damage. And if the event is shared via social media channels, it can escalate quickly.

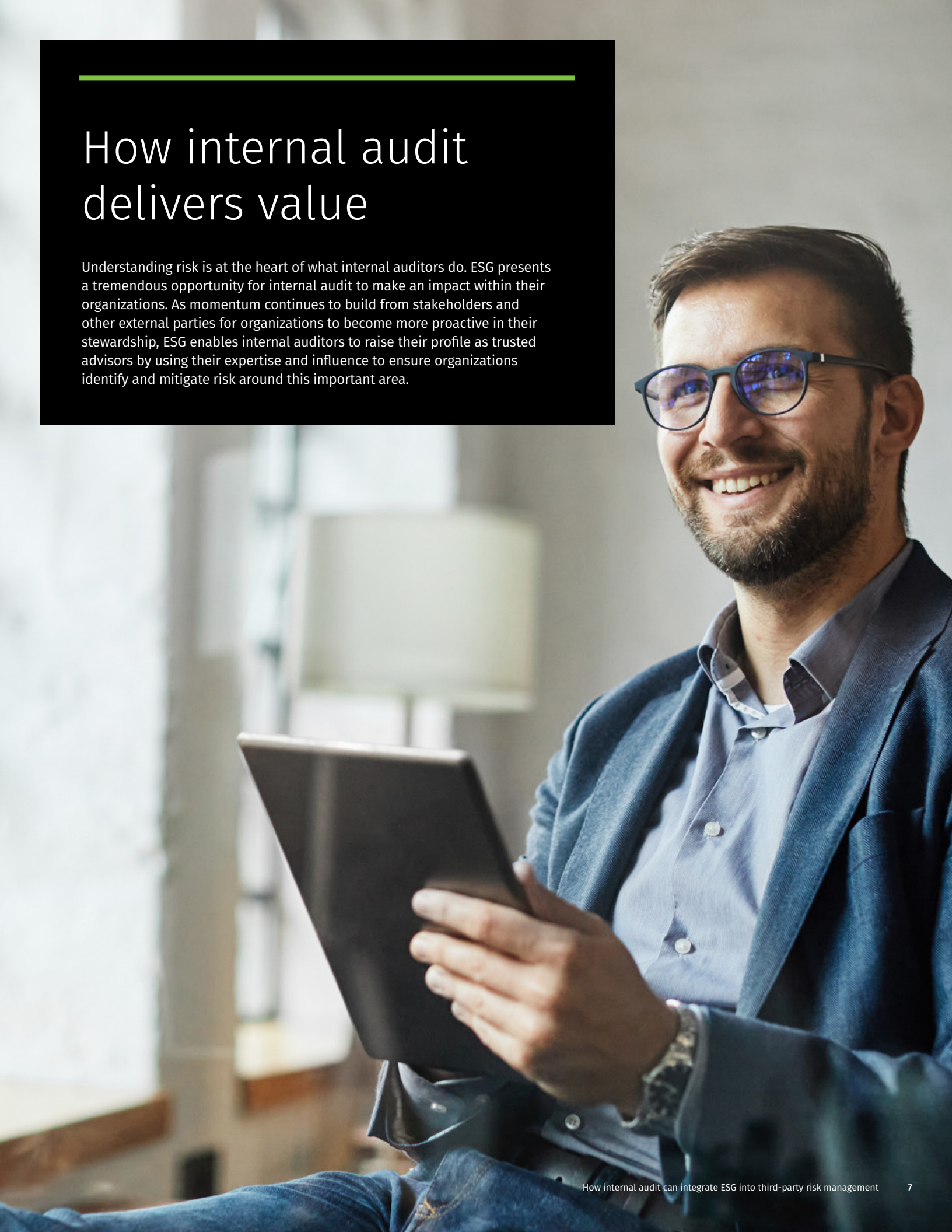
Internal audit teams can play an important oversight role in third party risk management. While they might not be making specific vendor management decisions, they should be involved in making sure proper due diligence is followed when selecting vendors. And once vendor relationships are in place, internal audit teams can monitor these arrangements to ensure organizations aren't opening themselves up to new risks and providing assurance that controls are operating effectively. Internal audit teams can help their organizations account for potential ESG risk by:

- Inventorying third-party relationships
- Mapping risks and controls
- Asking third parties to self-assess
- Identifying which third parties have data access
- Understanding if your third parties use third parties that could negatively impact your business

When it comes to ESG risk, it is not as straightforward as internal auditors might like. It will be impossible to understand how individual risks are impacted by third parties if you don't understand your own organization's ESG risk program. Review the vendor risk management policy and understand your organization's contracting process to ensure that ESG requirements are covered. Most importantly, know what dependencies, if any, on upstream or downstream providers and suppliers exist. The further away they are in the value chain, the weaker the controls become, and the more at risk your organization may be. By staying on top of evolving vendor management risks, internal audit teams can help their organization remain safe while getting the most out of their third-party relationships.

How internal audit delivers value

Understanding risk is at the heart of what internal auditors do. ESG presents a tremendous opportunity for internal audit to make an impact within their organizations. As momentum continues to build from stakeholders and other external parties for organizations to become more proactive in their stewardship, ESG enables internal auditors to raise their profile as trusted advisors by using their expertise and influence to ensure organizations identify and mitigate risk around this important area.



Contact information

Americas
4221 W Boy Scout Blvd #500
Tampa, FL 33607
U.S.A.
Phone: +1 800 449 8112

Europe, Middle East, and Africa
41st Floor
25 Canada Square
London
E14 5LQ
United Kingdom
Phone: +44 20 3197 6566

Asia Pacific
5 Shenton Way
#20-01/03 UIC Building
Singapore 068808
Phone: +65 6380 8000

Please visit **tm.wolterskluwer.com** for more information.

Wolters Kluwer