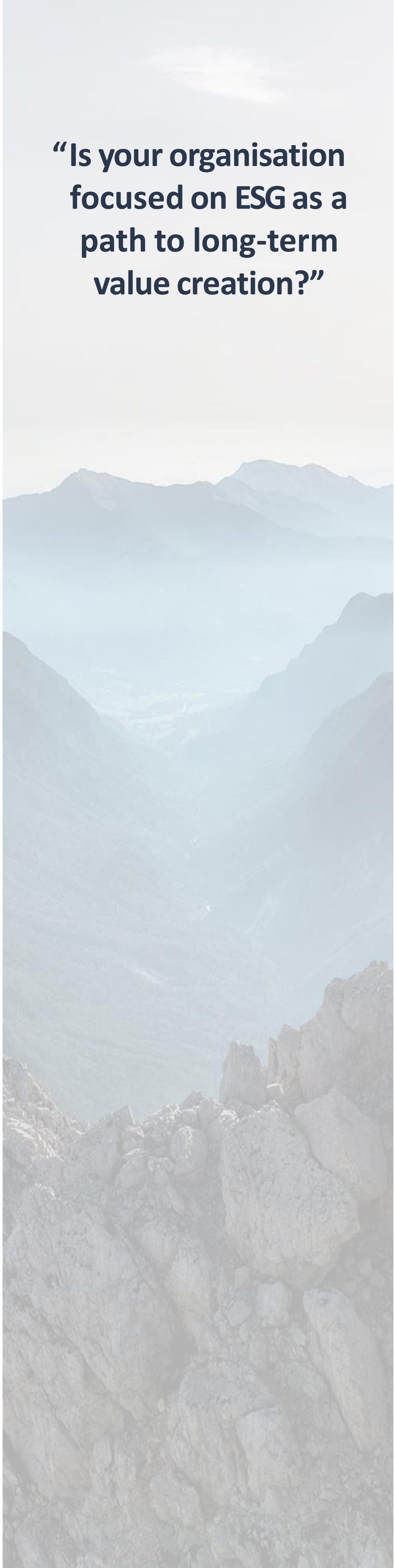
How to Audit Climate Risk Management

Key Considerations for Developing Climate-related Risk and Reporting Audit Strategy

Deloitte.

Table of Contents



“Is your organisation focused on ESG as a path to long-term value creation?”

Introduction

Global interest in environmental, social, and governance (ESG) issues, compliance, and reporting has grown dramatically since 2020. Against the backdrop of climate change impacts, social change movements, and the COVID-19 pandemic, consumers, employees, investors, governments, and other stakeholders reexamined and recalibratedtheir expectations for how businesses can be held accountable for responsible ESG performance.

Internal audit has a role to play in responding to this surge in demand for better ESG transparency. Understanding the individual components of ESG and where they do or don’t intersect is crucial to begin to understand the unique requirements for examining the veracity and completeness of ESG reporting.

Here’s how each of the component is defined:

“The **E**, or environmental, component of ESG information encompasses how a company is exposed to and manages risks and opportunities related to climate, natural resource scarcity, pollution, waste, and other environmental factors, as well as a company’s impact on the environment.

The **S**, or social, component of ESG comprises information about the company’s values and business relationships. For example, social topics include labor and supply-chain information, product quality and safety, human capital topics such as employee health and safety, and diversityand inclusion policies and efforts.

The **G**, or governance, component of ESG encompasses information about a company’s corporate governance. This could include information on the structure and diversity of the board of directors; executive compensation; critical event responsiveness; corporate resiliency;and policies and practices on lobbying, political contributions, and bribery and corruption”.

While ESG's environmental dimension has long enjoyed stakeholder focus, social and governance concerns also rose to the forefront. Now, even private companies are held up to a public microscope. Ethics, diversity and inclusion, human rights, labor practices, material sourcing and supply chain, access, data security/privacy — it's all fair game for public scrutiny.

Unsurprisingly, these changing stakeholder expectations are resulting in increasing demand for ESG transparency, accountability, and assurance. Globally, regulators are beginning to draft and implement more formal ESG performance standards. But many stakeholders are going a step further, pushing businesses to embrace ESG for value creation.

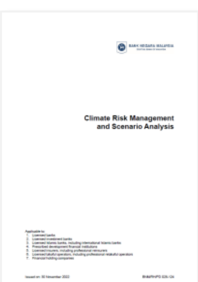
The overarching message is that mere compliance isn't enough. Consumers, capital investors, employees, and other stakeholders want businesses to integrate ESG considerations into the very core of how they do business. They want strong ESG value propositions and performance, and they are ready to withhold their business, funding, and support to ensure they get them.

Ultimately, regulators' reporting standards and frameworks will help you direct your ESG audit, risk management, and reporting activities. But it's up to your organisation to go the extra mile stakeholders are demanding. **Is your organisation focused on ESG as a path to long-term value creation?** Our guide to developing your ESG audit strategy can help you get on track.

Overview of the ESG Landscape

Malaysia's Regulatory Landscape on Climate Risk

In response to this increased financial impact of ESG on companies, financial reporting and accounting standard setters have made significant changes to their organisations to support the need for better reporting of both financial and operational metrics such as ESG. These new sources for reporting standards, corporate trends, and research are unambiguous. ESG is a significant driver of business performance now and into the future.


Climate Risk Management and Scenario Analysis

Bank Negara Malaysia

Climate Risk Management and Scenario Analysis Policy Document

Para 13.3: "Financial institutions shall **make annual climate-related disclosures** that are aligned with the recommendations of the Financial Stability Board's Task Force on Climate-related Financial Disclosures (TCFD) and shall be published together with **annual financial reports** for financial years beginning on or after **1 January 2024**."


MEDIA RELEASE

Bursa Malaysia

Bursa Malaysia Enhances Sustainability Reporting Framework with New Climate Change Reporting

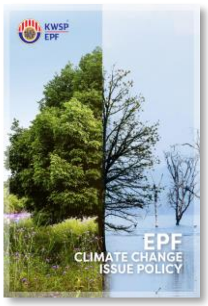
The Exchange recognises that listed companies require time to assess and respond to climate change-related risks and opportunities including putting in place the necessary policies, processes and practices. After a round of deliberations, the Exchange is now requiring **TCFD Aligned Disclosures** for companies starting from FYE **on or after 31 December 2025**.

Advisory Committee on Sustainability Reporting

Proposed National Sustainability Reporting Framework

Para 6.3: "Building on the existing sustainability reporting requirements, the potential approach for **adoption of IFRS S1 and IFRS S2 is for it to be made mandatory** for Main Market listed issuers. In addition, the reporting requirements may potentially be extended to include ACE Market listed issuers and large NLCos with annual revenue of RM 2 billion and above. This position may be expanded to other non-listed companies in the future. "

For Main Market listed issuers,
** IFRS S2 Reliefs shall be issued together with annual reports for FYE on or after **31 December 2025**.*
** IFRS S1 Reliefs shall be issued together with annual reports for FYE on or after **31 December 2026**.*
** Both standards shall be issued together with annual reports for FYE on or after **31 December 2027**.*



Employees Provident Fund

Priority Issue Policy: Climate Change

Core Requirement 11: "Companies should seek to **align their disclosures and reporting practices** relating to climate risks and opportunities with TCFD."

** Core requirements are expected to be met by companies **by 2024** and will follow a **"comply or explain" approach** in the case that companies require more time to comply with some of them.*

ESG Performance Is Business Performance

Before we dive into the nuts and bolts of how to drive ESG audit efforts, it's important to bring into focus the bigger-picture ESG business imperative of long-term value creation, as well as the stakeholder expectations that are driving it. As outlined by Deloitte in "Tectonic shifts: How ESG is changing business, moving markets, and driving regulation," consumers, capital investors, and employees alike "are looking for organisations to put purpose at the core of their operations, caring for the issues that concern their employees, communities, industries, and the world at large". Consequently, **the pursuit of stakeholder value and a healthy environment helps a business maximise its financial value.**"

In other words, ESG is being directly linked to business performance. As cited in Gartner's "2024 Audit Plan Hot Spots" —which pinpoints ESG as a top-ten risk area for internal audit department focus in 2024 — over the past years, double the institutional investors have committed to investing responsibly. They are incorporating ESG data into investment analyses and decisions. More creditors are issuing loans that adjust rates according to ESG performance. Employees and consumers are signaling they will end relationships with poorly performing organisations.

ESG Integration Required for Better Performance and Resilience

The charge is clear: Organisations need to build and integrate ESG performance and resiliencemetrics into their corporate reporting. They must prepare to disclose relevant, transparent, andhigh-quality ESG information and the resulting financial impacts. To enable these disclosures, they must employ the same financial reporting discipline and focus used for designing and implementing reliable, risk-based policies and processes that support effective oversight, internal controls, and assurance.

As we've discussed, organisations must also integrate ESG considerations in a way that driveslong-term value creation. So, let's start getting tactical: How can your organisation embrace ESG-driven business transformation to turn risk into opportunity? And how can you create reporting that reflects not only how your ESG efforts connect with each other and your finances, but also how they connect with value creation?

Deloitte's "The Sustainability Transformation" identifies three far-reaching strategies, advising:

Looking ahead.	Looking inside.	Looking around.
"Understand what threats and, more importantly, opportunities the pressures toward sustainability present for the future of the business".	"Consider how business operations could be reconfigured to accelerate the transformation toward greater sustainability".	"Leverage the surrounding business ecosystem to create competitive advantage".

What does that mean for your business? It may be time to widen and extend your perspective, thinking bigger and longer-term about how ESG is reshaping your industry, business model, and future. It may also be time to take a long look inside your organisation to see what you can do today to sustainably innovate products, services, and strategies in ways that facilitate growth and open up new opportunities. Finally, it's important to look for opportunities to strategically tapinto your broader business ecosystem. Can you engage external ESG capabilities or influence in ways that accelerate your organisation's ESGefforts? While your organisation likely has work to do in this area, you may have options to mobilise partner or vendor ESG capabilities, or to band together with other industry leaders to agree on and drive more sustainable business practices.

ESG Integrated Risk and Reporting Responsibilities

Roles across the organisation share responsibility to drive organisational alignment, manage ESG risk, and achieve ESG reporting, and value creation objectives. This includes not only obvious targets such as internal audit, board and executive leadership, risk, compliance, and sustainability, but also legal, HR, finance, strategy, operations, communications, and potentially others. It's vital that functions work together to harmonise ESG efforts, ensuring that the different roles aren't operating in silos. As such, an ESG risk and reporting program should not be implemented in isolation — it should be part of a larger, integrated risk management approach.

The graphic below showcases how the different roles work together in an integrated fashion, amounting to three different lines of defense supporting value creation from ESG efforts.

Figure 3. Value Creation From ESG Efforts

As illustrated in Figure 3, while the ESG program itself is the starting point:

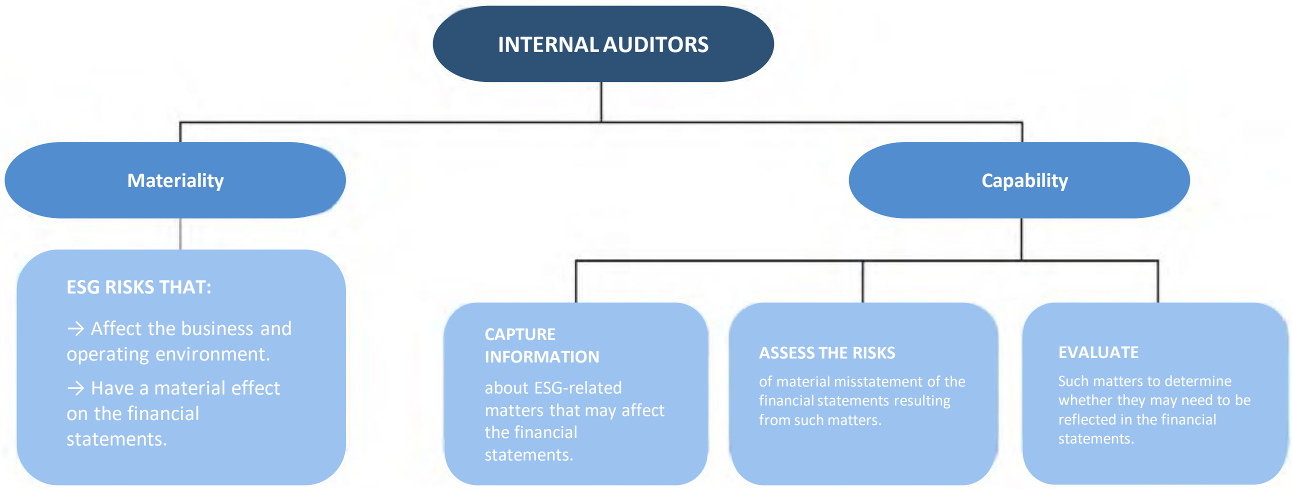
- The board, chief executives, and management act as a first line of defense by setting the wider ESG vision/strategy, establishing a "tone from the top", and driving urgency and accountability.
- Functional departments become the second line of defense by managing, monitoring, and mitigating ESG risk —owning data and maintaining responsibility for effective processes, controls, and policies supporting ESG risk management and reporting.
- Internal audit serves as the last line of defense, integrating ESG risk and compliance considerations into the audit plan while driving discipline and controls around material ESG risks. Internal audit is responsible for testing relevant controls and risks, advising on ESG reporting, and validating risk mitigation activities. Internal audit also plays a vital role inadvising the organisation on its broader risk management capabilities, and in anticipating and aligning efforts to emerging ESG risks, strategies, and organisational objectives.

What Internal Auditors Should Consider About ESG

Internal auditors also have a role to play. As noted in a Center for Audit Quality report on "Audited Financial Statements and Climate-Related Risk Considerations", companies are required to consider ESG-related risks "when the effect could reasonably be material to the financial statements." Internal auditors are required to perform risk assessments that include obtaining an understanding of the company and its environment. Those assessments must now consider the potential impact of ESG risks on the financial statements.

The International Auditing and Assurance Standards Board (IAASB) offers a practice aid on "The Consideration of Climate-Related Risks in an Audit of Financial Statement". Figure 4 offers a high-level illustration of the considerations for internal auditors.

Figure 4. ESG Considerations for Internal Auditors



ESG Internal Audit Planning Considerations

Just as with any other organisational risk, managing, monitoring, and reporting ESG risks and opportunities requires establishing a strong control environment within an effective governance structure. Internal audit should ensure that ESG is part of the risk conversation, incorporate ESG into the internal audit plan, and perform audits to provide assurance that the control environment is sound. The goal is to extend what you're already doing to incorporate ESG.

As your organisation gets focused on more effective ESG audit planning, the most importantstrategy is to ensure that you're asking all the appropriate questions.

Data Quality: Process Control and Governance

In particular, planning an effective audit of ESG requires an increased focus on data quality, asinternal audit strives to validate and assess the relevance, completeness, and accuracy of ESGrisk and reporting data. After all, the quality of your reporting is only as good as the quality of your data.

- What ESG data is the organisation currently reporting and to whom?
- How complex are the data or metrics? Where is it housed?
- What controls and processes support the data being reported? How does that fit into the internal audit plan? If it doesn't, how does it need to change?

Key ESG Forces Impacting the Traditional Internal Audit Approach

Begin identifying key questions for your internal audit plan by viewing activities in light of the unique ESG assertions impacting the traditional audit approach. These assertions require you to tailor your approach to the nature, extent, and timing of executing your audit plan. Alongside traditional applicable financial reporting assertions of completeness, accuracy, timeliness, cutoff, and understandability (clarity), unique ESG assertions include:

- **Balance** — Are you providing a well-rounded, balanced perspective on ESG activities? Are you identifying not only achievements and progress, but also limitations, weaknesses, and areas for improvement?
- **Stakeholder inclusiveness** — Who are your priority ESG stakeholders? Are you including them in how you contemplate ESG impacts? ESG stakeholders extend beyond capital market investors to employees, customers, consumers, and communities.
- **Sustainability context** — Are you providing reporting information within a framework that makes sense for your business, industry, and the related ESG impacts?
- **Prioritisation** — What ESG topics are most important for your organisation to focus on? How are you thinking through potential ESG risk impacts? How does that thinking guide your ESG strategy, governance, and disclosures?

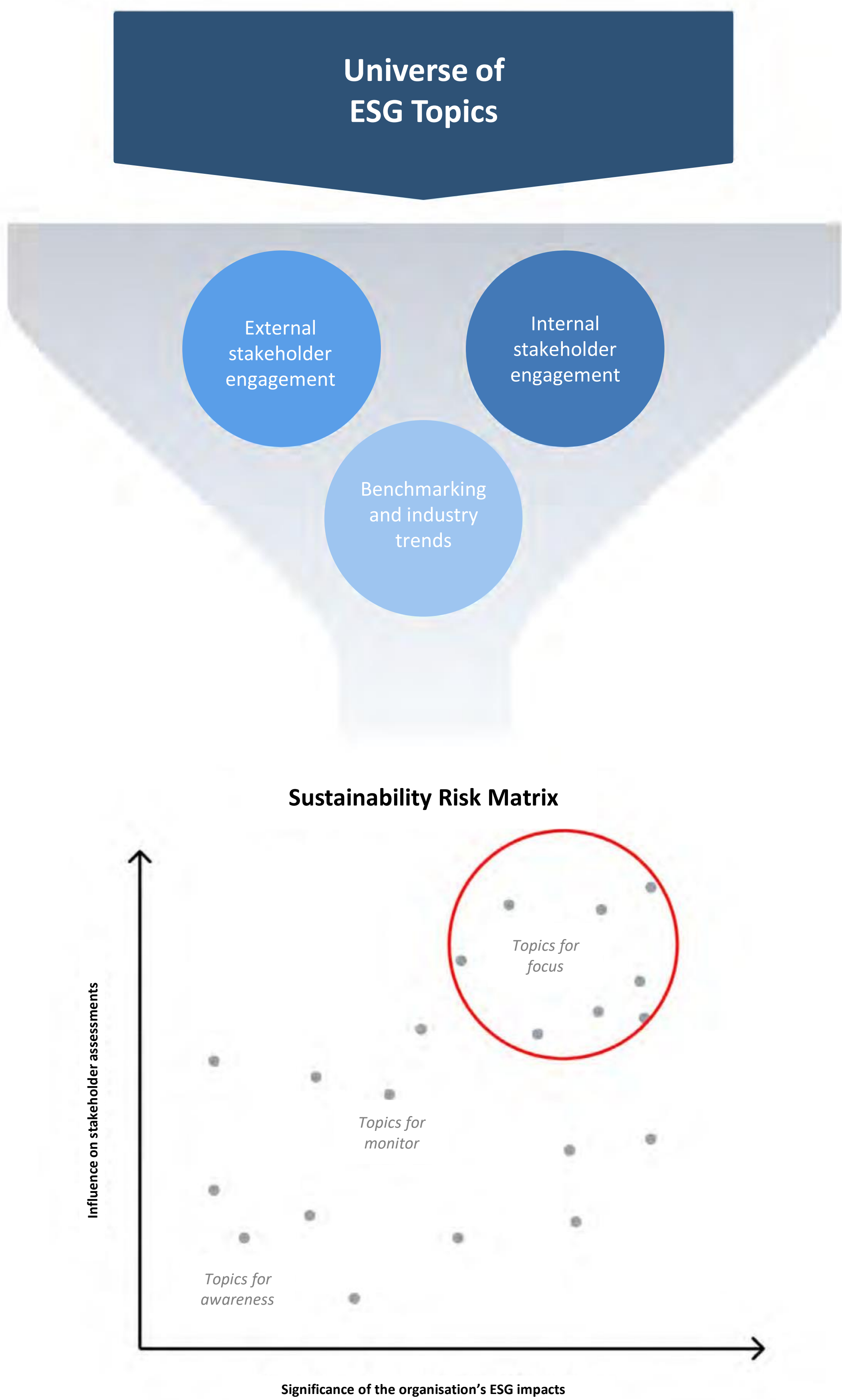
A Risk-Based Approach to Auditing ESG Risk and Reporting

Limited resources and accelerated reporting timelines require a tailored risk assessment grounded in meaningful criteria. Taking a risk-based approach helps to drive the selection and prioritisation of ESG focus areas. It's helpful to begin by filtering ESG topics through a lens of stakeholder engagement, industry trends, and benchmarking. From there, the higher-risk areas for your audit response are those where:

- Impacts are the most significant if ESG objectives are not achieved.
- Influence on stakeholder assessments is highest.

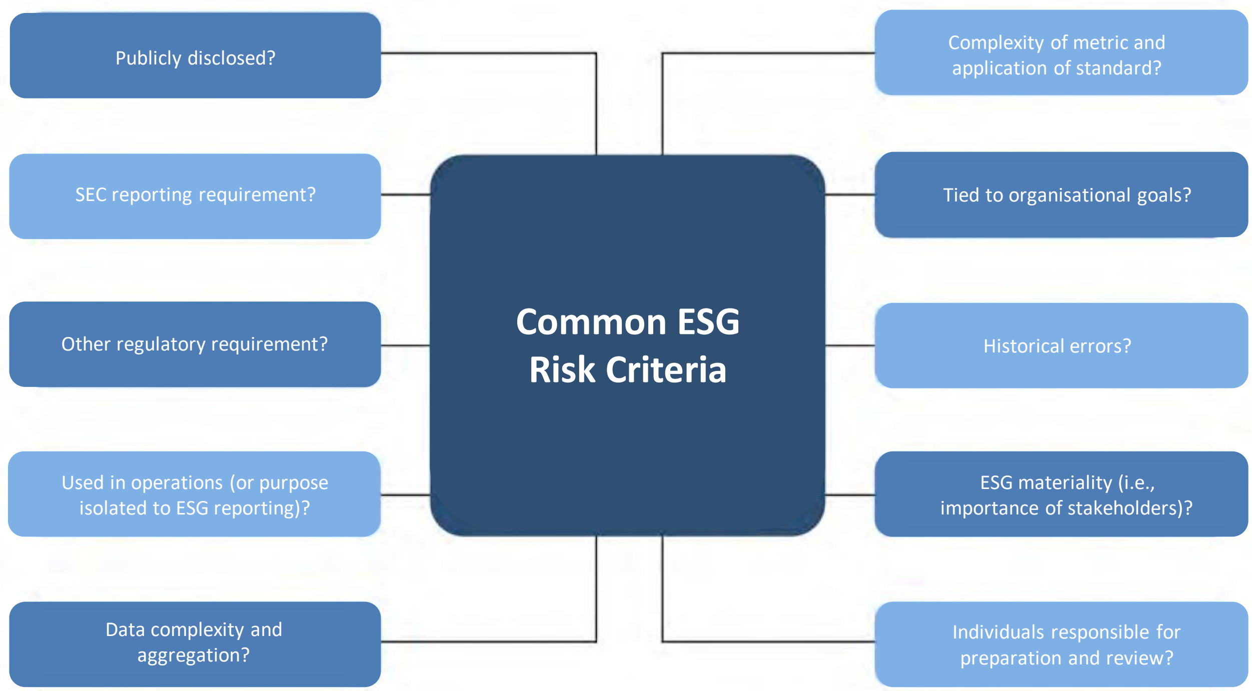
In other words, what matters most to stakeholders? And how does that overlap with your most significant impacts? For many companies, this is a process called a "materiality assessment" undertaken to help determine ESG focus areas for strategy and disclosure. The graphic below illustrates the high-level materiality assessment process that culminates in a relative prioritisation of ESG topics to consider.

Figure 5. ESG Risk Assessment Process



Once these material topics are identified, there are additional considerations to a risk-based approach to auditing ESG. The graphic below provides several common examples of ESG-focused criteria you can apply alongside existing risk-based criteria.

Figure 6. Sample Criteria for Assessing ESG Risk and Reporting



Common Approaches to Integrating ESG Risk and Reporting in Internal Audit Plans

Bearing these considerations in mind, how can your organisation best integrate ESG activities into its internal audit plan? The answer depends on several factors, including the maturity of your organisation and processes, your location, the industry in whichyou operate, and your ESG risk strategy and appetite. The most common approaches are described below.

Figure 7. Incorporating ESG Into an Internal Audit Plan

Standalone Reviews

Certain elements of your ESG program may be mature enough for internal audit to assess in standalone reviews. These assessments can help organisations understand their ESG policies, control landscape, and responsibilities at a specific point in time. For example, is the appropriate executive sponsorship in place? Are the necessary resources being made available? Are project plans in place to ensure implementations are being done according to plan, and at the appropriate level of detail and specificity? Is the source data substantiating that all ESG disclosures are complete, accurate, andreadily available?

Focused Reviews

For ESG areas of high stakeholder concern or low-risk appetite, organisations may wish to undertake more focused reviews. These deep dives can provide valuable assurance in key ESG areas, acting as more traditional audits that help to ensure policies, processes, and otherindividual ESG program elements are operating as they should. Focused reviews are likely to become more common as regulators begin to require specific ESG disclosures.

Focused reviews can include larger sample sizes over a longer period of time. Internal audit teams may layer in periodic checkpoints, such as six-month check-ins or quarterly updates, to ensure that action or mitigation plans are implemented and issues are effectively remediated. In other cases, however, internal audit teams may perform the focused review, identify findings, and leave it to management’s discretion whether to remediate issues, providing no oversight or follow-up.

Integrated Audit Approach

When ESG program elements are not mature enough for standalone assessments, organisations should consider the integrated audit approach. This approach can be used aspart of any audit as a pulse check on the business that provides reasonable assurance thatESG-related activities are being appropriately identified, considered, and documented.

Getting started with an integrated audit approach may be as simple as adding ESG-focusedquestions into the planning documents or checklists used by your internal auditors. Your fundamental objective in adding these questions is to begin gaining an understanding of where potential risks and opportunities lie throughout the organisation.

Investing in ESG Competencies

Many ESG issues represent significant risks and costs if not properly managed. Early investment in ESG can mitigate these risks — and even create new opportunities for growth and innovation. According to the 2023 AuditBoard's survey, 60% of organisations do not perform internal ESG audits, but 26% plan to in the next year — indicating that organisations intend to build out their ESG assurance efforts. And about two-thirds of the survey respondents have not implemented ESG controls, highlighting a low state of maturity in ESG data governance.

Your organisation may need to invest in ESG competencies by devoting resources to:

- Research and monitor ESG regulatory guidance and updates.
- Understand ESG risk and reporting trends and frameworks in your industry.
- Benchmark ESG topics in your industry.
- Assess internal and external stakeholder engagement in ESG topics.
- Build ESG knowledge through targeted training or via certifications such as the Global Reporting Initiative's Professional Certification Program or Competent Boards' ESG Certificate Program.

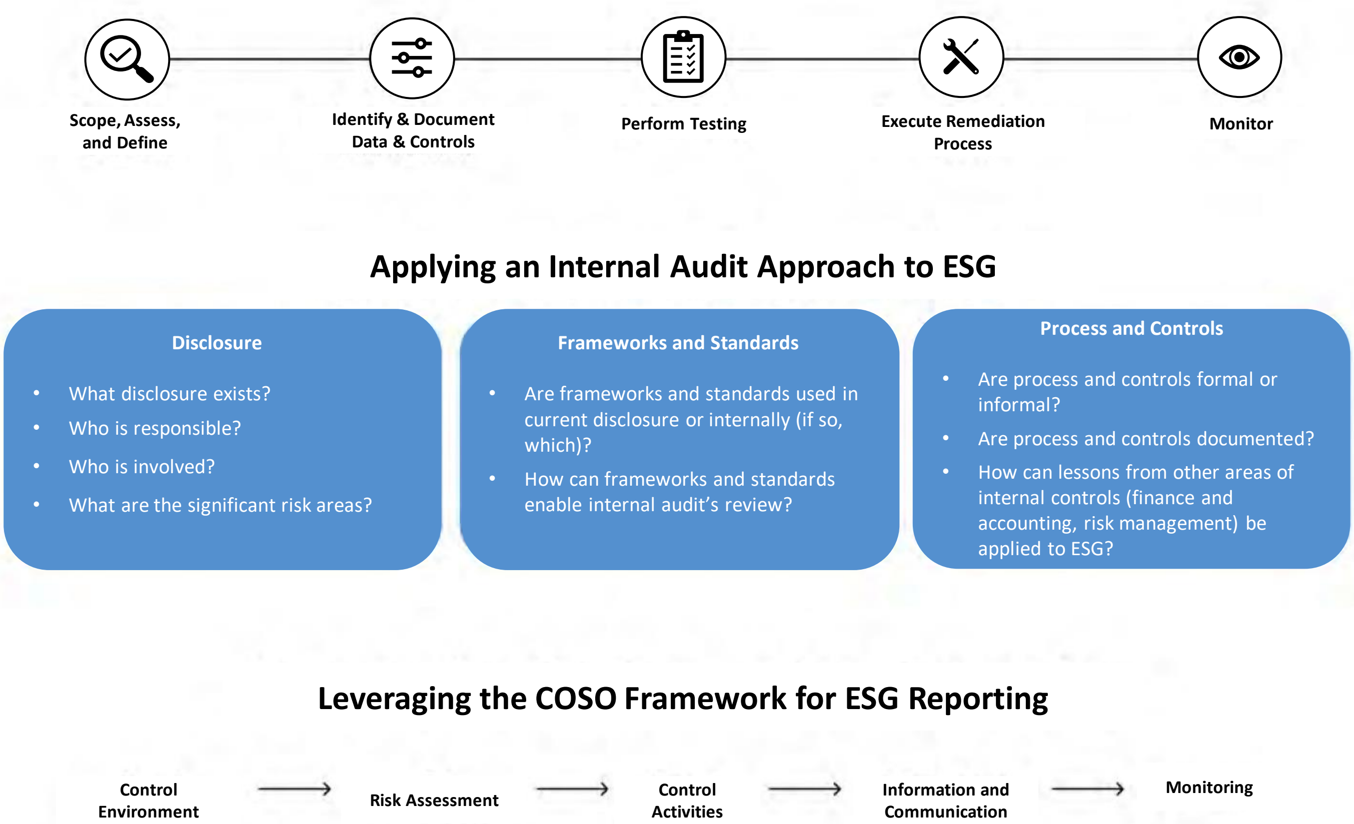
As you determine how best to invest in ESG competencies, begin by looking inside your organisation for professionals who are motivated to upskill in this area. Internal audit skill sets already bring a foundation of professional skepticism and experience with other transformational change initiatives — a solid foundation for springboarding into ESG. Identify professionals to help you develop your capabilities, and work together on a plan to build needed expertise.

Illustrative Internal Audit Plan and Approach

The illustrative plan below begins to bring together these different components, getting tactical about how organisations can apply the discipline, structure, and rigor of internal auditto ESG. While at this time there is significant interpretation involved in assessing ESG topics, internal audit can begin to simplify judgments by:

- Extending the methodologies traditionally applied to auditing financial reporting to ESG,and directly integrating ESG reporting with financial reporting.
- Viewing ESG efforts through a lens of disclosures, frameworks and standards, and processes and controls.
- Understanding that ESG will be implemented throughout the entire internal audit life cycle, from annual and ongoing risk assessments, audit planning, and audit execution through to reporting and ongoing monitoring.

Figure 8. ESG Reporting Internal Audits



ESG Internal Controls: Leveraging the COSO Framework

Your ability to manage ESG risk and reporting depends largely on the design and effectivenessof your internal controls. Without effective controls, you cannot assure the data quality required to provide accurate, meaningful ESG reporting. Many organisations, however, do not yet have robust, reliable controls around ESG data.

As we've outlined, the solution may be better integration of ESG with risk management and financial reporting. What might that look like in practice? "Leveraging the COSO Internal Control-Integrated Framework to Improve Confidence in Sustainability Performance Data", a whitepaper produced by individual authors from SASB and the Institute of Management Accountants (IMA), offers perspectives and strategies on how this can be done.

The essential idea is that the Committee of Sponsoring Organisations (COSO) Framework can help organisations apply the same rigor to ESG (i.e., how ESG information is measured, managed, and validated) typically applied to financial reporting. The authors' goal is to help organisations better use, assure, and communicate ESG data while emphasising professionaljudgment and stakeholder learning.

As indicated in Figure 9, the COSO Framework requires five components. Though the guide offers more detailed discussion and case studies, below is a summary of the relevance of each to ESG audit activities.

COSO Element	Relevance for ESG Internal Audit Approach
Control Environment	• Setting a "control" consciousness (typically from management and the board) that guidesESG reporting objectives while setting the stage for the processes and discipline neededto govern controls. • Establishing the organisation's commitment to creating structures that provide ethical, independent, sustainable, and accountable oversight of internal controls development and performance.
Risk Assessment	• Guiding with clear objectives that support the identification and analysis of specific ESGrisks to the achievement of organisational objectives. • Considering both internal and external stakeholder needs. • Identifying and assessing changes impacting internal controls (e.g., regulatory changes,M&A, geographical exposures, tech rollouts).
Control Activities	• Establishing policies and procedures to create activities that effectively mitigate or manage identified ESG risks. • Tailoring all activity types appropriately when practical.
Information and Communication	• Gathering or generating timely, relevant, and reliable ESG data to support effective functioning of internal controls. • Verifying that appropriate performance measures (e.g., Key Performance Indicators, or KPIs) and communication processes are in place to describe and share ESG information both internally and externally. • Using risk assessments to guide selection of the most important ESG factors to monitorand disclose.
Monitoring	• Using review activities (separate from reviews performed as control activities) to support the organisation in assessing whether all COSO components are present and functioning. • Employing ongoing evaluations built into business processes, periodic separate evaluations (e.g., conducted by internal audit), or independent third-party reviews. • Communicating deficiencies in a timely manner to those responsible for corrective action.

What Lessons Can We Take From Existing Assurance Framework to Help Provide Assurance Over ESG?

Much like the existing assurance frameworks that have taught us to establish effective internal control governance related to financial reporting, upcoming ESG-related legislation and regulatory requirements will necessitate a similar level of transparency. Consider applying these common activities to clearly define, assess, and track the impact of climate risks, including against specific financial metrics.

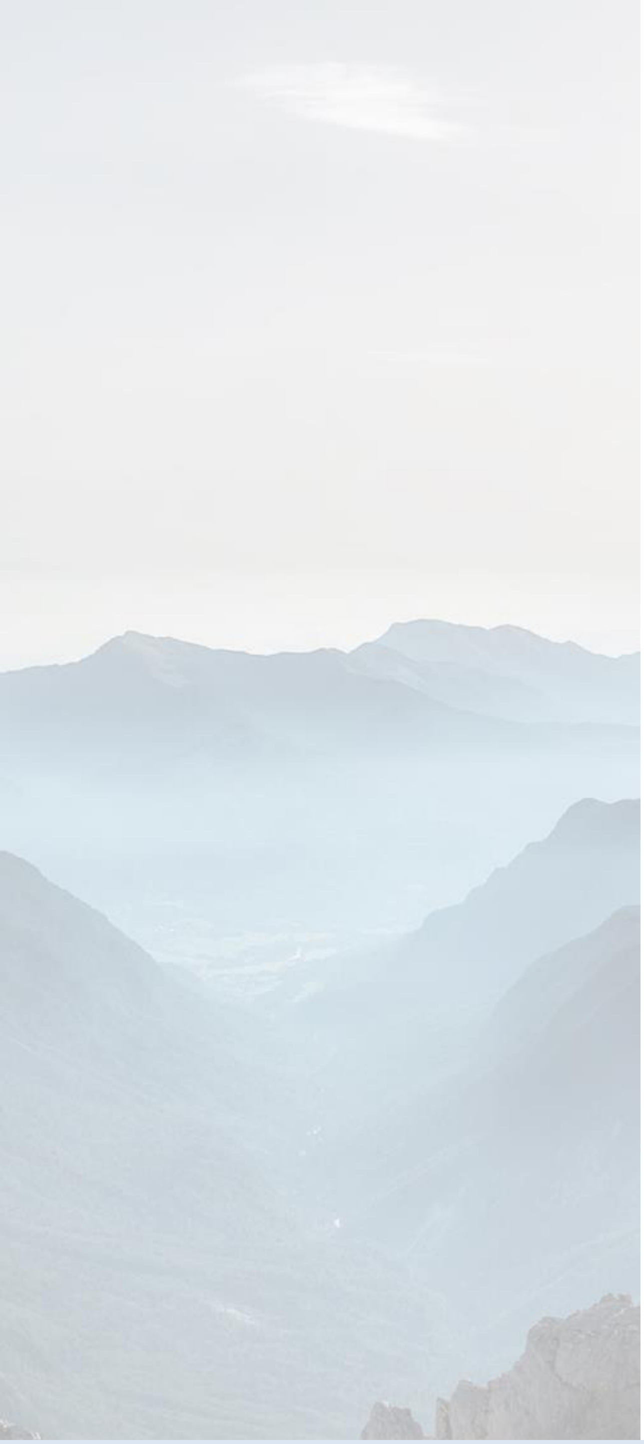
- Identification of material balance sheet accounts.
- Mapping material accounts to underlying processes.
- Identifying key controls and secondary controls for those processes.
- Documenting the processes and controls with walkthrough narratives, flowcharts, and risk/control matrices (RCMs).
- Identifying applications and IT general controls (ITGCs) that support the processes and controls.
- Capturing a risk assessment of the ESG environment.
- Defining your organisation's level of required assurance covering internal controls over ESG.
- Training for control owners, reviewers, and internal auditors that includes discussion about the cultural mindset across the organisation.
- Providing reporting to senior management.

In addition to the above activities, the following section will discuss how implementing enabling technology is a crucial step to facilitate testing, review, and issue remediation efforts.

Getting Started: Questions for Assessing ESG Risk

Ready to take action to better understand your organisation's ESG risks and opportunities? The questions below offer a starting point for your internal audit function to assess risk across the enterprise. If your organisation collaborates with other organisations, you may also wish to use these questions to begin assessing their ESG risks and opportunities.

Key questions for a risk-based approach to auditing ESG	
Governance and policy	• Has the organisation created a governance structure and culture that supports effective ESG risk management? • Has the organisation defined a strategy to strengthen internal awareness and commitment, emanating from top management (setting the "tone at the top")? • Is information on ESG risk being reported to the board?
Risk strategy and appetite	• Are ESG strategy and risk appetite consistently cascaded through the organisation, including limits and metrics? • Are ESG-related risks being considered in new products and services? • How has ESG and the changing external business environment affected the resilience of the business model and hence the risk strategy?
Risk assessment, measurement, and analytics	• Has the organisation defined a consistent, comprehensive methodology for ESG quantification? • Has stress testing been adapted to reflect the long-term horizon of ESG risk?
Monitoring and reporting	• What ESG-related disclosures around governance, strategy, risk management, KPIs, and KRIs are being published? • How is ESG risk monitoring and reporting being aggregated into existing risk practices?
Portfolio and capital management	• Are there potential capital add-ons that are associated with integrating ESG risk into existing risk management frameworks? • Are there portfolios of ESG risk-related products and services to manage?
Risk data and systems	• Is there readily available, consistent, credible, and sufficiently meaningful data? • What are the "new" data elements that will be required for the organisation, as well as for its suppliers, borrowers, and other third parties?
Risk operating model, people, and culture	• Has ownership and accountability for ESG risks been determined, and is it linked with other risk types? • How is the organisation monitoring and understanding the complex and evolving regulatory landscape? • How is the organisation attracting and retaining resources with ESG skill sets?



Conclusion

Whatever your organisation's ESG risk managementand reporting status and expected ESG impact, the imperative is to get started. Required disclosures are expected, and internal and external stakeholders alike are directly tying ESG to business performance. Businesses can no longer deny that ESG issues are financially material.

That's why value-driven organisations are taking a proactive approach to understanding the current andevolving impact of ESG issues on their businesses. Byfocusing on shaping the more sustainable, equitable, and responsible business models, governance frameworks, strategies, products, and behavioural changes stakeholders are demanding, they're positioned to turn ESG challenges into opportunities for long-term value creation.

Planning a more effective internal audit strategy that incorporates ESG risk and reporting is an important step towards moving down the appropriate path — but **your organisation must also prepare to go a significant step further, directly connecting ESG efforts with value creation**. That means not only embedding ESG into ongoing risk and reporting activities, but also committing to a bigger vision that incentivizes true transformation — helping you become a more sustainable, resilient organisation capable of delivering lasting financial and business value.

Connect with us

Dr. Chee Wei Yen
Executive Director
Deloitte Risk Advisory
wechee@deloitte.com

Lloydon Leong
Director
Deloitte Risk Advisory
llleong@deloitte.com