Internal audit's role in sustainability/ESG

Financial Services
Banking and Capital Markets, Asset Management and Insurance

Issue 1

kpmg.com

Supporting your ESG goals

Environmental, social, and governance (ESG) issues are becoming increasingly relevant. Banks, Asset Managers and Insurers (collectively, financial services organizations) understand that embracing ESG will allow them to raise capital, secure talent, strengthen the employee value proposition, and attract loyal customers. ESG has gone from a nice-to-have to an integral piece of long-term financial success.* As a result, sustainability is generating a new type of risk: ESG risk. Financial services organizations have begun reimagining their governance structures over ESG, creating steering committees composed of executive leadership and making strategic decisions about commitments, actions, and disclosures.** Financial services organizations are also adjusting business risk strategies and corresponding risk appetite statements—making sure roles and responsibilities are fully transparent throughout all three lines of defense. Internal audit can play a critical role in providing objective assurance and advice on ESG reporting and sustainability matters more broadly.

Environmental

considers how an organization performs as a steward of nature. This can include issues related to financed emissions, waste management, water management, and climate change vulnerability.

Social

examines how organizations manage relationships with employees, customers, and the wider community. Risks that fall under this category can include corporate social responsibility, labor management, data privacy, general security, health and safety, and well-being.

Governance

refers to variables such as business ethics, board and leadership, executive pay, audits, internal controls, intellectual property protection, and shareholder rights.

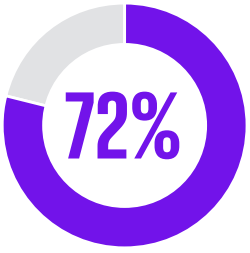
*Stakeholders want clarity and details regarding ESG strategies and initiatives. For instance, how are banks managing existing portfolio companies as it relates to those companies' carbon footprints and plans to better manage those demands. Further, stakeholders may want more concise information on such issues as bank's plans for investments in renewable energy or nuclear power businesses. It is important to note that increased shareholder value could be tied to ESG disclosures and performance against ESG goals.****

* KPMG International, 2022 CEO Outlook, August 2022

** KPMG International, 2022 Survey of Sustainability Reporting, September 2022

*** KPMG 2022 U.S. CEO Outlook, August 2022

Source: 2022 Banking Industry Survey – Navigating in Choppy Waters



of banks disclosed climate change as a financial risk that will impact their business in the longer term

Source: "Climate risk is financial risk – For banks it's a board-level issue," KPMG LLP

Regulatory, investor, and stakeholder pressure

Many stakeholders across the globe see financial services organizations as a major lever in addressing sustainable development goals and combating climate risk. Regulatory bodies are paying close attention and Securities and Exchange Commission (SEC) regulations are underway. As a result, financial organizations like banks, asset managers, and insurers will come under greater pressure to reorient their capital to sustainable activities.

Great ESG expectations

ESG has become an imperative. ESG strategy has become necessary to address stakeholder requirements and regulation as well as to build competitive advantage, improve resilience, and drive value. Its impact is profound and a critical factor for financial services organizations that want to be ready for fundamental changes that are coming. For example, many asset managers have raised, or are raising, funds for pure-play ESG/ Impact investments. More generally, ESG considerations are being woven into investment due diligence processes, mutual fund product options for customers and new insurance coverages. An ESG focus is increasingly becoming a baseline expectation for investors and those committing capital.

"No regrets" moves

Financial services organizations understand the need to pivot towards more sustainable investing and lending but still have significant books of business wrapped up in lending to "high emission" assets or general account investments of insurers, for instance. As these assets continue to generate profits, financial firms will have to find a way to balance their duty to finance the transition against their fiduciary duties to shareholders.

As with financial reporting, the independent and objective assurance that internal audit can provide must be an integral part of an organization's ESG response.

Objective insights and advice on ESG matters

Internal audit is in a unique position within the organization to provide guidance, add value, and leverage its experience to provide an efficient approach in implementing change. Providing guidance around operationalizing ESG strategies and goals in a manner that can be subject to internal controls in the wake of upcoming changes is an imperative. According to the Institute of Internal Auditors, internal audit has clear roles in providing assurance and advisory ESG services that may include the following:

Assurance

- **Internal audit's undeniable role in ESG reporting:** ESG systems and controls should have adequate time to mature and have internal audit's first look prior to facing inevitable external auditor scrutiny. Internal audit can also help ready your sustainability and governance metrics, processes, and related controls to get ahead.
- **Review reporting metrics for relevancy, accuracy, timeliness, and consistency:** Providing public ESG reports (nonfinancial) information that accurately depicts an organization's ESG efforts is critical. Any conflicts with formal financial disclosures will raise a red flag with investors and regulators and are particularly important as regulatory oversight and public scrutiny increases.
- **Conduct materiality or risk assessments on ESG reporting:** Organizations' ongoing ESG efforts or public commitments to reaching ESG goals can quickly give rise to higher levels of materiality.
- **Incorporate ESG into regular audit plans:** Internal audit has deep corporate knowledge (culture, ethics, governance frameworks and processes, and their related risks) and should come to recognize ESG-related assurance engagements in the future.

Advisory

- **Identify areas that are less well-defined and build an ESG control environment:** Internal audit can initiate discussions that are not quite ready for assurance, involving regulatory guidelines or expectations, and advise on developing specific internal controls for ESG reporting.
- **Recommend reporting metrics:** Internal audit can provide insights into the kind of data that accurately reflects relevant ESG efforts within the organization.
- **Advise and advocate on ESG governance:** Internal audit can provide guidance on ESG governance vendor due diligence and advise on tools, technologies, and information technology (IT) infrastructure due to its holistic understanding of risk across the organization and advocate for the company to approach ESG risk in a thoughtful manner.

KPMG

Internal audit can support management in answering the following questions:

- Do we have a clear view of all ESG risks and opportunities, including compliance risk related to existing and upcoming SEC and regulatory expectations, and are those regularly reassessed?
- Are we prepared for these upcoming legislative and regulatory expectations?
- Do we have a data inventory of all ESG metrics being disclosed?
- Do we have sufficient IT infrastructure?
- Do we have a proper ESG culture and risk management that goes hand in hand with our ESG goals and strategies?
- What are our ESG public commitments today and do we have policies, procedures, controls, and data to support these public commitments?
- Can you say today that your organization has an effective risk and compliance program for ESG?
- Are ESG considerations embedded within the organization's principal risk stripes?

Credit risk | **Operational risk** | **Compliance risk** | **Liquidity risk** | **Market risk** | **Reputation risk** | **Strategic risk** | **Human capital risk**

ERM Risk Practices: https://advisory.kpmg.us/articles/2023/esg-risk-practices.html

ESG journey

Internal audit can play a critical role in each phase of a company's ESG journey.

Assess
Identify current state of ESG initiatives

Deep-dive assessment

- Maturity and materiality
- GHP inventory
- ESG data
- Risk and opportunity
- Reporting readiness

Roadmap

Operationalize
Design and implement tangible initiatives for specific focus areas to increase value

Target setting and decarbonization	ESG due diligence
Resilence	Valuation and modeling
Reporting automation	Governance
SOX-like internal controls	Data measurement
Transition planning	Methodology and policy creation
Systems implementation	On-call services

Change and program managament

Report
Issue consistent, comparable, reliable, and assurance-ready reporting

- Accounting
- Reporting
- Disclosure

Assurance

Key drivers

Stakeholder opinion

Stakeholders, customers, employees, and other stakeholders linking climate to risk management, value creation, and brand reputation

Regulations

Rising regulatory expectations and/or mandates in areas of climate risk management, governance, board/management accountability, and reporting

ESG internal audit methodology

Internal audit's ESG mandate should go beyond simply identifying risks and preventive controls. It should include ensuring linkage among strategy, governance, and risk management to ensure internal controls are working efficiently throughout the organization. Our ESG internal audit approach combines different elements of our established internal audit methodology supplemented by our experience in ESG.

Key ESG categories

Internal audit coverage

Transition risks

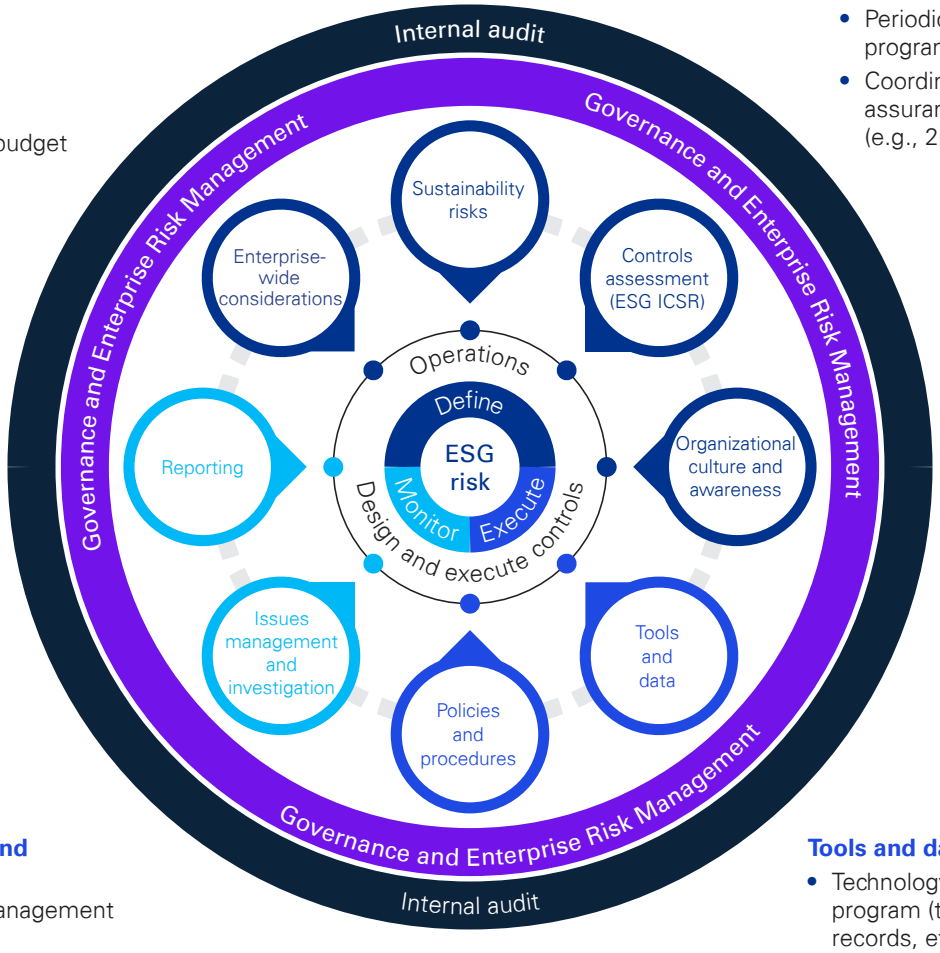
- Changes in policy and regulation
- Technological improvements
- Changes in consumer demand physical risk
- Acute weather events
- Chronic changes in climate

Enterprise-wide considerations

- Definition of ESG
- Mission, vision, values, and strategy
- Periodic review by top management
- Context and stakeholder analysis
- Time, resource, and budget

Controls assessment

- Monitoring and tracking of regulatory change
- Process and control testing
- Periodic AESG risk program evaluation
- Coordination with other assurance providers (e.g., 2nd line)



Reporting

- SEC and regulatory reporting
- Periodic reporting to management and the board
- External reporting to stakeholders
- Record keeping

Organizational culture and awareness

- Engage and create dialogue with all the stakeholders
- Culture/tone of ESG/sustainability and behavioral
- change
- Regular and frequent training and communication

Issues management and investigation

- Issues/complaints management and remediation
- Responding to regulatory examination/inspection
- Response plan and process for investigating alleged noncompliance
- Continuous improvement

Policies and procedures

- ESG policy existence and management
- Entity-wide policies and procedures (human capital, health and safety, cyber, lending and credit practices, investments, etc.).
- Consistency between policy framework and strategy

Tools and data

- Technology to support ESG program (testing, training records, etc.)
- Predictive measures: key risk indicators and key performance indicators
- Root cause analysis and trending
- Data governance/management

Service offerings: How can KPMG help?

KPMG's Internal Audit methodology is flexible and can be tailored to each company's specific needs. Internal audit service offerings can range from examining aspects of the company's ESG governance policy such as high-level oversight, risk assessment, due diligence procedures, and awareness to assessment of controls in place to support existing ESG commitments. The suite of assessments identified below can be separately performed or executed in phases as part of an overall readiness ESG assessment.

ESG governance assessment	Internal controls over sustainability reporting	ESG in internal audit
Objectives		
Assess the organization's ESG governance structure in alignment with the COSO 2013 framework. Assessment may include consideration of the following: • Board oversight and committee structures • Materiality assessment review • Policies and procedures • Strategy to link identified ESG risks to a company's business imperatives, including its business model • Operational plan implementation (target operating model implementation)	Identify published ESG commitments and metrics along with an assessment of controls, policies, procedures, and data to support external ESG reporting: • Assess ESG commitments and metrics against peers and regulatory expectations. • Assess entity level and ESG reporting processes and controls. • Assess whether policies, procedures, and controls are in place to help ensure incorporation of climate and cyber risk considerations to help ensure complete and accurate reporting of key metrics, including regulatory reporting considerations for metrics impacted by recent SEC proposals, such as climate greenhouse gas emissions and cybersecurity.	Develop/design tactical steps for implementation of an internal assurance model over ESG reporting and setting course for embedding ESG into the internal audit function: • Support preliminary ESG risk assessment to help determine areas of focus. • Assist internal audit functions in embedding ESG considerations into their audit universes and plans. • Support reporting strategy, policies, processes, controls, people, technology, data, etc, to achieve overall readiness. • Support processes around ESG diligence, including assessment over alignment with investment mandates.
KPMG accelerator		
ESG governance framework with leading practices underpinned by the COSO 2013 Internal Control Framework and TCFD.	Metric risk assessment methodology and risk accelerator toolkit for a set of common metrics, including process flows, RACIs, and risk and control matrices.	ESG operational risk templates, such as audit programs, risk assessments, and audit reports.
KPMG deliverables		
• Gap Assessment Report against COSO ESG governance control framework	• Prioritized risk metrics and goals inventory • Process workflows • Risk and controls matrix • Internal assurance model and guiding principles	• Audit Program Guide for common ESG risk areas • Audit report template • Internal audit risk and control matrix
Market drivers		
Federal and state regulatory expectations as well as the SEC proposed rules and EU regulatory bodies are looking at the following: • How financial services organizations oversee governance of ESG risks • How ESG-related risks are identified • How they materially impact a business' strategies, models, and outlook • Investment portfolio alignment with ESG commitments • Climate assessment based on product offerings. These qualitative elements, if adopted as proposed, can have far-reaching impacts in formalizing how they govern, monitor, measure, analyze, and report ESG activities.	Many companies voluntarily assess and report on their ESG commitments. A primary concern, however, has been the resulting lack of standardization across definitions, data, and established controls to support these commitments. In addition, proposed mandatory financial and nonfinancial ESG metric disclosures by the SEC and increasing regulatory scrutiny have emphasized the need to ensure a robust control environment to support the accuracy of these disclosures. Also, the Federal Reserve Board is conducting a pilot climate scenario analysis exercise that includes six of the largest financial institutions designed to enhance both supervisors' and firms' capabilities for measuring and managing climate-related financial risks, further demonstrating the need for robust ESG controls.	An executive order has directed federal agencies to develop and execute strategies to quantify, disclose, and mitigate climate-related risks to the assets of public and private entities. Regulators are taking action to address climate risks within their supervisory frameworks. There are some initial expectations regarding the use of tools in assessing the links between climate risks and economic outcome, such as climate scenario analysis and risk modeling.

Multidisciplinary approach

We have access to a wide range of ESG competencies, assets, and solutions. This broad ESG lens requires a multidisciplinary team. KPMG has a one-stop-shop approach to help ensure that the right professionals are engaged to support our clients.

Experience

Our team of subject matter professionals, with experience in internal audit as well as ESG, has the skills and knowledge to provide innovative internal audit services that meet varied needs across a wide range of industries.

Contact us

TJ Scallon
Partner
Internal Audit and Enterprise Risk - Financial Services Lead
KPMG LLP
T: 646-300-0085
E: tscallon@kpmg.com

Aila Pallera
Principal
Internal Audit and Enterprise Risk - Financial Services
KPMG LLP
T: 818-571-1165
E: cpallera@kpmg.com

Jason Freund
Partner
Internal Audit and Enterprise Risk - Insurance
KPMG LLP
T: 973-876-0006
E: jfreund@kpmg.com

Eric Carlsson
Managing Director
Internal Audit and Enterprise Risk - Asset Management
KPMG LLP
T: 973-214-6769
E: ecarlsson@kpmg.com

Michael A. Smith
Partner and U.S. Internal Audit Solution Lead
KPMG LLP
T: 469-441-8831
E: michaelasmith@kpmg.com

Steve Estes
Partner and U.S. Internal Audit ESG Lead
KPMG LLP
T: 972-896-9476
E: sestes@kpmg.com

Special thanks to Rachel Horne, Justin Kitts, and Matthew Musgrave for their supporting contributions.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia