

# COMPLIANCE INSIGHTS



## What Role Should Compliance Play in ESG?

*By Bernadine Reese and Jackie Sanz*

Regulators and many other stakeholders are intently focused on how financial institutions address environmental, social and governance (ESG) matters. Within financial institutions, boards of directors, executive management and much of the C-suite are weighing in on the ESG strategy and approach. Chief compliance officers (CCOs), though, have been remarkably silent. This void raises the obvious question “What role should Compliance play in ESG?”

The ESG agenda is bold, combining three key and far-reaching topics — each of which, on its own, presents significant compliance challenges for financial institutions. For example, at the United Nations’ Conference of the Parties in 2015, many governments committed to using financial objectives, and the global financial system, to achieve global climate-change goals and targets. The size and complexity of the response required — by some estimates \$6 trillion per annum will be required to fund the changes needed to achieve net-zero carbon emissions, with 80% of that coming from private sources<sup>1</sup> — have resulted in more than 1,000 mandatory laws, disclosure requirements and regulations, which have broad impact on global financial institutions.<sup>2</sup>

<sup>1</sup> Paris Agreement, United Nations Framework Convention on Climate Change, 2015, [https://unfccc.int/sites/default/files/english\\_paris\\_agreement.pdf](https://unfccc.int/sites/default/files/english_paris_agreement.pdf).

<sup>2</sup> Sustainability Reporting Instruments Worldwide, Carrots & Sticks, [www.carrotsandsticks.net/reporting-instruments/?status=Forthcoming&status=Current&esgCoverage=Environment&esgCoverage=Governance&esgCoverage=Social&mandatoryVoluntary=Mandatory](http://www.carrotsandsticks.net/reporting-instruments/?status=Forthcoming&status=Current&esgCoverage=Environment&esgCoverage=Governance&esgCoverage=Social&mandatoryVoluntary=Mandatory).

Legal and regulatory considerations aside, there are also sound commercial reasons to adopt an ESG strategy. In a 2021 survey, 76% of consumers across various geographies said they will stop buying from companies that treat the environment, employees or the community in which they operate poorly.<sup>3</sup>

Responding to the demands of their various stakeholders, including regulators, shareholders, employees and the general public, financial institutions have made ESG commitments across the spectrum of ESG to which they will be held to account. To achieve their goals, financial institutions will need to integrate ESG considerations into almost all areas of their businesses and will need to make periodic disclosures on their progress.

We see chief financial officers (CFOs), chief risk officers (CROs), chief sustainability officers (CSOs) and other C-suite executives shaping ESG strategies, but CCOs are often missing from these discussions. Why is this, and does it make sense?

## The key challenges of implementing ESG requirements

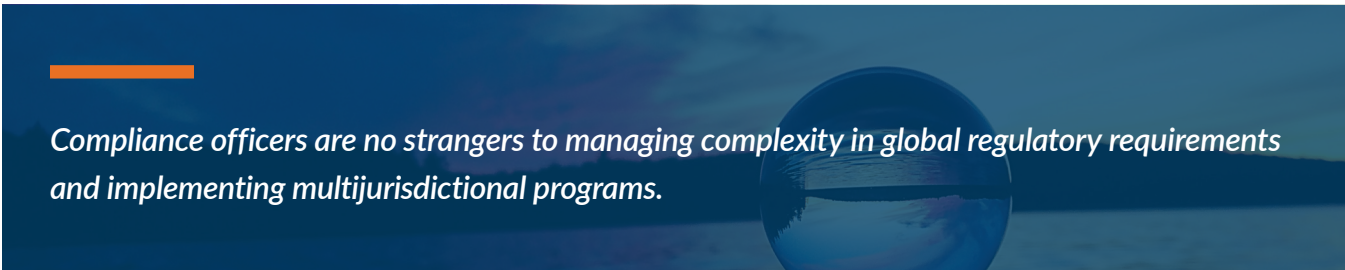
The importance of engaging CCOs in ESG discussions is highlighted by the key ESG regulatory risks:

- **Breadth of mandatory new E regulations and requirements:** Given the acceleration of new environmental regulations, it is a challenge keeping up. In the 2021 survey, 37% of respondents cited a lack of reporting standards and regulatory/complexity, and 31% cited volatility of regulatory requirements as barriers to ESG progress.<sup>4</sup> Following on from government green strategies, ESG requirements cover a broad range of topics, including an initial focus on entity-level reporting and disclosures, product taxonomies and disclosures, scenario analysis and modeling, and sustainable finance and the development of green products.
- **Scope of S and G requirements:** As with environmental requirements, S and G requirements have developed or are developing along national and, in some instances, local lines:
  - The development of legislation and regulation for the S dimension of ESG has been maturing over many years and includes measures to combat human trafficking and modern slavery; labor laws and employment rights; diversity, equity and inclusion; and other human rights initiatives. Defining the scope of these requirements across different countries, and determining the enterprise approach, can be challenging.

<sup>3</sup> *Beyond Compliance: Consumers and Employees Want Business to Do More on ESG*, PricewaterhouseCoopers, 2021, [www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/consumer-and-employee-esg-expectations.html](http://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/consumer-and-employee-esg-expectations.html).

<sup>4</sup> *Beyond Compliance*.

- While many would argue that G requirements and expectations for financial institutions are long-established, the form they take varies significantly from formal G regimes, such as the United Kingdom’s [Senior Managers and Certification Regime](#) and Australia’s [Banking Executive Accountability Regime](#), to more directed (e.g., limits on compensation) and less formal regimes.
- **Divergent rules and requirements:** As ESG requirements have evolved, they have not been consistently developed or internationally aligned:
  - Regulatory requirements vary by country, and the same disclosure requirements can be based on different underlying calculations. In addition, the laws of some countries apply across jurisdictions, such as the European Union’s [Corporate Sustainability Reporting Directive](#) (CSRD), which can apply to non-EU-based companies, and the [European Sustainability Reporting Standards](#), which will become the baseline for CSRD compliance.
  - Requirements vary by line of business, so the allocation of capital by banking activities (e.g., capital raising, lending and trading) attract different requirements than asset management activities.
  - Some requirements (such as those of the International Sustainability Standards Board (ISSB)) apply between jurisdictions, whereas in the United States, intrajurisdictional requirements mean there may be variations between state-level and federal ESG laws.
  - Differing regulatory requirements, frameworks and standards are complicated by varying implementation timelines and, in some cases, whether adoption is voluntary or mandatory.
- **Implementation complexities:** While there are many complexities, especially noteworthy are the following:
  - Impact across the organization – ESG requirements impact all areas of the business. Assessing the material implications and determining an appropriate risk management and reporting strategy require a coordinated approach, appropriate governance and strategy and coordinated leadership from multiple teams.



*Compliance officers are no strangers to managing complexity in global regulatory requirements and implementing multijurisdictional programs.*

- Customers, supply chains and third parties — ESG requirements include an assessment of impacts, and reporting from customers, supply chains, and third-party vendors and partners. For example, data must be collected for disclosure of Scope 3 emissions, and the social impacts of an organization’s supply chain and third parties must be assessed and managed from a regulatory and reputational risk perspective.
- Data — ESG reporting requires significant external data, which brings challenges such as availability, reliability, consistency, comparability and relevance. Environmental data may include science-based targets, emissions reporting or carbon accounting, introducing unfamiliar data sets and calculations for financial institutions.

In addition to specific legal and regulatory requirements, financial institutions have undertaken voluntary commitments. It is estimated that 42% of financial institutions globally have committed to reduce Scope 1 and Scope 2 greenhouse-gas emissions to net zero by 2050, and the Global Financial Alliance for Net Zero has secured net-zero commitments from more than 550 financial institutions, representing \$150 trillion in assets.<sup>5</sup>

Many other commitments have been made in other areas of sustainability, green finance, diversity and inclusion, human rights, and other social and development goals. Globally, there are various initiatives, such as the Climate Policy Initiative’s Net Zero Finance Tracker, charting progress toward these targets. As the focus shifts from voluntary commitments to mandatory requirements, regulators are expecting financial institutions to report on progress toward achieving these targets, and the reputational risk of making misleading or exaggerated sustainability-related claims (i.e., greenwashing) could be considerable.

What we have is an evolving, complex and disparate agenda — regulatory and discretionary — that financial institutions must be able to manage effectively. Who in the organization has the most experience tackling such a massive undertaking? The obvious answer is the CCO, as the organization’s Compliance leader. While Compliance has this experience, it can’t and shouldn’t own the ESG program. Rather, it should collaborate with and guide the business in its response. As we discussed in our [December 2022](#) issue of *Compliance Insights*, compliance teams are broadening their risk mandate to many areas that involve various risk and process owners across the organization. ESG is another example of this trend.

<sup>5</sup> “Financed Emissions Are Missing From Many Firms’ Net Zero Plans,” S&P Global, January 20, 2023, [www.spglobal.com/esg/insights/financed-emissions-are-missing-from-many-firms-net-zero-plans#:~:text=The%20data%20shows%20that%2042%25%20of%20banks%2C%20financial,the%20785%20financial%20institutions%20assessed%20in%20the%20CSA.](https://www.spglobal.com/esg/insights/financed-emissions-are-missing-from-many-firms-net-zero-plans#:~:text=The%20data%20shows%20that%2042%25%20of%20banks%2C%20financial,the%20785%20financial%20institutions%20assessed%20in%20the%20CSA.)

## What does Compliance bring to ESG?

Compliance officers are no strangers to managing complexity in global regulatory requirements and implementing multijurisdictional programs.

Many organizations manage ESG issues across multiple business units without a coherent set of comprehensive standards and guidelines around risk-assessment approaches, taxonomy, data collection and analysis, and governance structures. Several business units with ESG issues to manage lack the experience and skills to deal with mass emerging and evolving regulatory requirements and the heightened regulatory scrutiny that accompanies them. The scrutiny that comes with the transparency of granular ESG-related data will be particularly important to address.

Compliance teams are often tasked with thinking strategically about regulatory risks and applying risk-based approaches and impact assessments in engaging with relevant stakeholders to understand challenges. They have extensive experience in understanding and navigating such challenges, while keeping their finger on the pulse of industry peers and competitors to appropriately benchmark activities undertaken.

Strong, comprehensive governance is important with cross-functional compliance initiatives and in situations where regulatory obligations are evolving and at different maturity levels across multiple jurisdictions. Compliance teams also bring independent regulatory challenge to the business, operational and governance processes by asking tough questions and through monitoring and testing activities. This feedback is key to successful ESG implementation.

Compliance can assist with strategic prioritization of activities to address systematic risks — through the innovation of solutions and development of controls — to avoid the risk of repeat deficiencies. Compliance is well-versed in identifying and mitigating material risks, including identifying reasonable risks to knowingly accept, and in eliminating risks that have punitive financial and reputational consequences.

### Greenwashing

Regulatory scrutiny and enforcement action regarding promotional practices have increased in many jurisdictions, with greenwashing being an obvious target. Compliance, as part of its business-as-usual monitoring activities, will need to integrate ESG considerations. For example, the scope of marketing and sales communications will expand beyond ensuring that disclosures are not misleading and are supported by appropriate records to evaluating ESG-related claims. This broader scope will include ensuring that there are no instances of greenwashing and that messaging is supported by fact and aligns with associated regulatory-based disclosures.

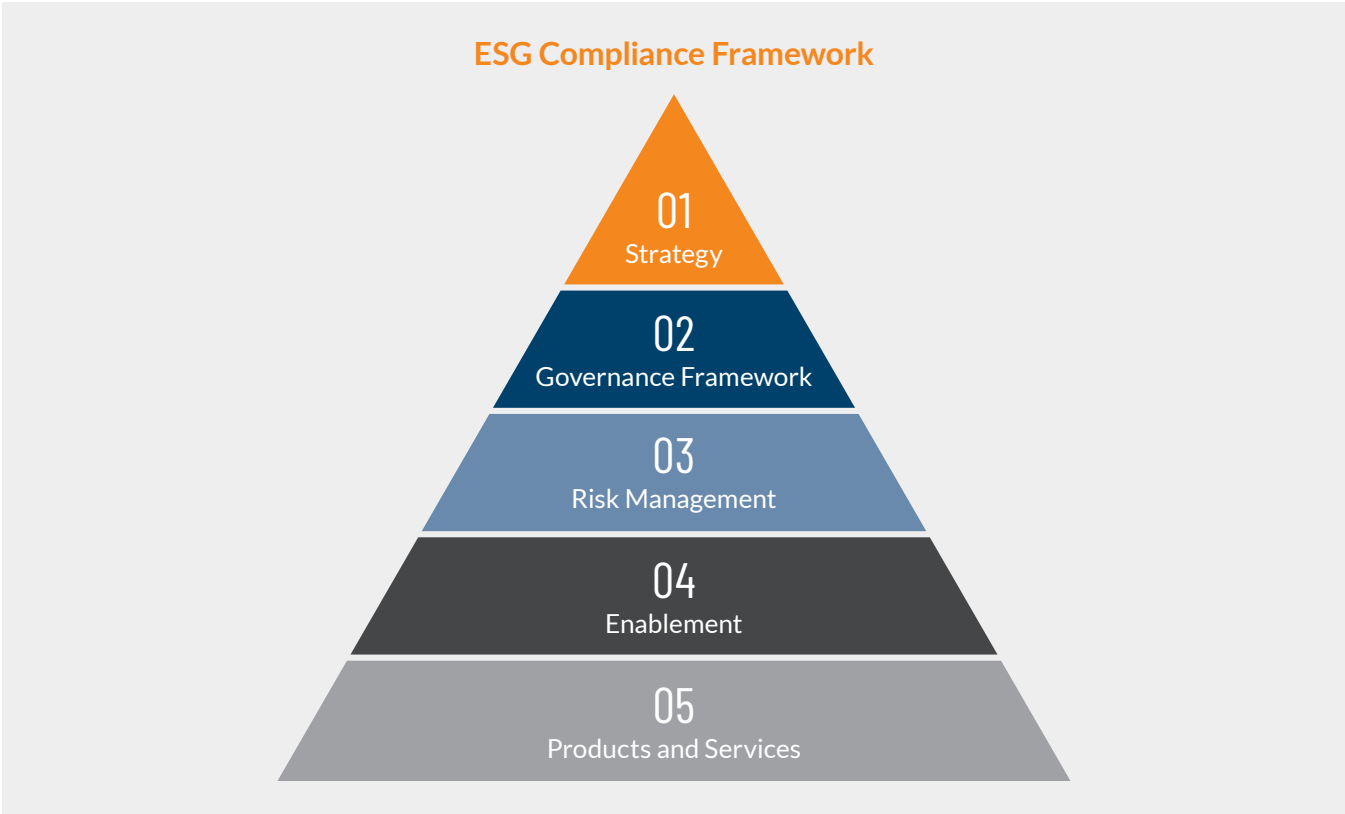
Regardless of its role in ESG strategy, Compliance will be monitoring the regulatory risk associated with ESG obligations. Rather than advising on remediation activities after deficiency identification, Compliance should provide challenge to strategic decisions and, as with other regulatory risks, be viewed as a trusted adviser to the risk owners. The function should ensure that the risk of regulatory deficiency is appropriately mitigated within the organization’s established risk-tolerance limits.

It is vital for Compliance to be involved now. Regulatory expectations are increasing, and managing regulatory and reputation risk will become ever more important.

### Defining Compliance’s Role in ESG

As noted above, Compliance should not assume responsibility for the ESG program – it is not the risk owner. The risks are owned by various business functions across the organization. Compliance plays an important role in the governance and oversight structures of a financial institution and, as with other regulated activities of an institution, should have a seat at the table. The compliance team can provide line of sight across activities of the organization because of its intimate familiarity with the processes and key regulatory risk controls throughout the operations of the business.

To ensure ongoing compliance with a growing number of ESG-related regulations, a holistic framework for identifying, measuring, managing and reporting ESG risks and mitigation strategies is needed. The framework should incorporate at least five elements of the ESG program:



Compliance teams should be engaged in each of the above elements, with a mandate for the following tasks:

- Ensure that the strategy is incorporated across the institution's regulatory footprint.
- Assist in the materiality assessment needed to identify relevant ESG factors to be incorporated into an organizationwide taxonomy.
- Liaise with CFOs, CROs, CSOs and other C-suite executives to develop a coherent ESG strategy and plans that can be consistently communicated to regulators and meet regulatory expectations.
- Ensure that the ESG strategy and organizationwide initiative aligns with the organization's overall risk appetite and tolerance levels.
- Provide insight and advice in the development of the governance structure, ensuring that all compliance facets (e.g., reporting, escalation, roles and responsibilities, legal entity management, three-lines-of-defense considerations, subject-matter experts (SMEs), etc.) are integrated.
- Help define regulatory and reputational risk and provide insights on risk mitigation approaches, including a risk-based approach to implementing ESG requirements that ensures proportionality.
- Assist in development of a comprehensive regulatory database, including processes to identify and integrate emerging regulation.
- Adapt the organization's existing policies and procedures to ESG regulatory changes, including in impacted areas such as marketing and investment advice.
- Assist and advise on compliance risk management activities, including the control-effectiveness assessments integral to measuring residual risk and evaluating risk-appetite alignment.
- Participate in enablement activities, including identifying data requirements, key risk indicators and key performance indicators, and tools and technology to support risk management and governance activities.
- Advise on the institution's cultural and ethical responsibilities and strategies for their execution.
- Incorporate ESG requirements in assessments and evaluation of regulatory risk in product and services governance frameworks.
- Support ESG health checks.

Compliance teams are experienced at performing risk assessments of various types of compliance risk. ESG compliance is a new risk factor to consider in the process and should be applied across multiple functional areas of the organization (e.g., third-party risk management, procurement, marketing, product or service design, finance and accounting). The results of the risk assessments will factor into the compliance monitoring and testing activities.

Ongoing effectiveness of the compliance team in the ESG initiative requires an inward review and assessment of the team. The CCO should immediately:

- Evaluate whether the team's structure is impacted by the need to integrate ESG activities into the compliance team's activities (e.g., develop and/or add SMEs within existing teams, create a separate team of SMEs, etc.).
- Conduct an ESG skills assessment of the existing team and consider training needs.
- Build ESG-specific monitoring and testing activities into the annual compliance plan.
- Establish roles and responsibilities of the team within the institution's ESG framework (e.g., within the governance activities and risk management activities, and as part of the enablement activities supporting ongoing compliance).

## **What are the next areas of focus for ESG?**

Greater regulatory alignment over the upcoming months is likely as international bodies such as the International Organization of Securities Commissions and the ISSB attempt to bring together existing frameworks and standards. However, complexity will remain a key issue in ESG. Compliance will need to have a greater role in navigating emerging ESG topics such as:

- Integrating ESG considerations into third-party risk management, supply chain, and procurement relationships and activities, as well as location and premises strategies and plans.
- Assessing ESG risks in relation to customer acceptance, and onboarding and gathering data and information to support assessments of sustainability and social risks.
- Integrating ESG assessments into business decisions, including lending and credit reviews, investments, fund and discretionary mandates, insurance and reinsurance strategies, and funding, as appropriate.
- Integrating ESG considerations into other risk assessments to ensure that decision-making takes account of all risks.
- Maturing governance arrangements, including consideration of ESG objectives and goals within performance assessments, remuneration and compensation arrangements.



- Balancing litigation risks with progress toward ESG objectives and implementation.
- Designing sustainable finance products to meet market demand and assessing the financial promotions of these products to avoid accusations of greenwashing.
- Considering the S definition, materiality assessments and policy development.
- Keeping pace with increasing regulatory disclosures and changes to the E agenda as regulations shift from climate change to broader world impacts (e.g., biodiversity).
- Continuing to mature, develop and keep pace with ESG data needs, provisions and risks to ensure that disclosures and reporting meet industry best practices.

## Conclusion

Compliance officers have a big role to play in ESG implementation initiatives in financial institutions and can contribute meaningfully in the efforts to implement effective policies, procedures and risk assessments. Many in compliance functions want to make a difference and play a key part in the ESG transformation that is just starting. The knowledge, skills and experience of compliance teams mean that it is vital that they step forward and bring this understanding to bear in ESG.

## About the Authors

**Bernadine Reese** is a managing director in Protiviti's Risk and Compliance practice. Based in London, Reese joined Protiviti in 2007 from KPMG's Regulatory Services practice. Reese has more than 30 years' experience working with a variety of financial services clients to enhance their business performance by successfully implementing risk, compliance and governance change and optimizing their risk and compliance arrangements. She is a Certified Climate Risk Professional.

**Jackie Sanz** is a managing director in Protiviti's Risk and Compliance practice. Based in Toronto, Sanz has been the chief compliance officer, chief privacy officer, chief anti-money laundering officer and senior complaints officer of an international asset manager and fund company with locations in Australia, Canada, Hong Kong, Ireland, Peru, Singapore and the U.S. She has also played the same role for a Canadian trust company. Sanz spent three years in Luxembourg focused on société d'investissement à capital variable (SICAV)/fonds commun de placement (FCP) for offshore distribution as well as Cayman Islands and British Virgin Islands funds.

## About Protiviti's Financial Services Industry and ESG Practices

Protiviti's Global Financial Services Industry practice has served 80% of the world's largest banks and many of the largest and mid-sized brokerage and asset management firms, as well as a significant majority of life, property and casualty insurers. The FSI practice provides support to teams across Protiviti's portfolio of solutions, including regulatory compliance, risk management, internal audit, technology, cybersecurity, data privacy and sustainability.

Protiviti's ESG practice offers expertise and support across multiple ESG topics, using our ESG framework outlining challenges, risks and opportunities, and stakeholder impacts. Our ESG framework informs our approach to helping institutions and enables a holistic approach tailored to institution-specific requirements. Protiviti's ESG practice can support institutions with ESG assessments, including ESG frameworks, ESG data management, ESG internal controls and ESG capability maturity assessments.

---

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.