# CSRD reporting requirements place Compliance function in the spotlight

*Rebecca Kozlowski, Serap Tutkun and Laura Schroder-Van Oorschot*[1]

**The Corporate Sustainability Reporting Directive ('CSRD') requires an estimated 50,000 companies in the European Union ('EU') to report on a wide range of Environmental, Social and Governance ('ESG') topics and puts the compliance function in the spotlight. Many companies may be unaware that their existing Compliance function activities may already address some of the CSRD requirements, such as Anti-Bribery and Corruption ('ABAC') training and risk culture. However, most companies will have gaps to resolve or may be struggling to determine their reporting information under CSRD. Those companies should look towards their compliance programs and integrated control frameworks, as they can support in the transition.**

## 1. Introduction

The scope of Compliance continues to expand within the Netherlands and wider European Union ('EU') as more extensive and onerous regulations are developed. Whether related to third party risk management or data protection, the Chief Compliance Officer ('CCO') has often been the person responsible when change is introduced. One such regulation is the Corporate Sustainability Reporting Directive ('CSRD')[2], which requires an estimated 50,000 companies to disclose qualitative and quantitative information regarding a wide range of (non) financial risks, including traditional compliance risks, such as corporate culture, treatment of employees, Anti-Bribery and Corruption ('ABAC') and respect for human rights. Most companies should (therefore) recognize the compliance risks identified by CSRD as already addressed by their integrated control frameworks and associated compliance programs.

A sound integrated control framework includes compliance and environmental, social, governance ('ESG') risk assessments and associated controls, as well as monitoring, testing, and reporting of those risks, controls, and compliance activities. A comprehensive compliance program supports the control framework through various elements related to prevention, detection, and response. Regulatory change such as the CSRD requires sound integrated control frameworks and mature compliance programs to embed new requirements without negatively impacting the companies' risk culture and overall achievement of objectives.

Training & communication and governance & culture are core to the success of a compliance program.[3] These are two areas where CSRD requires disclosure; specifically, via the European Sustainability Reporting Standards ('ESRS') which are (draft) standards for companies to use when determining the breadth and depth of detail expected for the CSRD disclosures within their annual reports.
This article seeks to provide insight into how existing compliance programs and integrated control frameworks should be used to support the transition to and execution of the CSRD reporting. While various compliance program elements directly relate to the ESRS, the focus of this article is placed on one element of compliance programs and one ESRS: governance & culture and ESRS G1 Business conduct. We will also provide guidance on where to begin if you believe that your company is not (yet) compliant with the CSRD. Lastly, we will explain why a cross-functional approach that includes CCOs is important for a successful implementation.

1. Rebecca Kozlowski, Senior Consultant, KPMG Forensic Integrity & Compliance. Serap Tutkun, Senior Manager, KPMG Forensic Integrity & Compliance. Laura Schroder-van Oorschot, Senior Manager, KPMG Capital Markets Accounting Advisory Services.
2. EUR-Lex - 32022L2464 - EN - EUR-Lex (europa.eu)
3. Groen, L. et al. (2022). The state of ethics and Compliance in the Netherlands – 2022 Chief Compliance Officer Survey results. KPMG Netherlands. Retrieved from: https://kpmg.com/nl/en/home/insights/2022/02/the-state-of-ethics-and-compliance-in-the-netherlands.html

## 2. Risk culture is an important building block of the CSRD

A sound risk culture within a company often proves to be the key to success. Culture influences ethical conduct, employee involvement, innovation, and compliance awareness. In doing so, it contributes to achieving the strategic objectives of a company. Culture that is not well embedded has been linked to many historic incidents of loss, fraud, or corruption. This has led to integrity and compliance awareness receiving increased (public) attention.

Companies are becoming more and more explicit in pursuing an honest culture and being compliant with the relevant laws and regulations. This pursuit means that they have a growing need to obtain insight into the current level of compliance awareness and risk culture within their company. There is a powerful business case for a strong risk culture and compliance awareness due to countless scandals and incidents globally, and management and supervisory boards increasingly see this as vital to implementing purposeful strategies to create value for all stakeholders. Research shows that a good risk culture can deliver, amongst others, an improvement in financial performance, an enhancement in the ability to innovate and an improvement in staff engagement and retention.
To create a strong risk culture and a compliance awareness, it is important to pay attention to soft controls that have a real or potential effect on ethical conduct Employees need to feel free to express and discuss doubts and dilemmas and maintain and/or improve their skills and knowledge. This requires continuous and specific attention. One way to do this is to invest in training and education, which in turn will improve compliance awareness and ethical conduct by employees. Training and education are tools that companies should use to implement their controls and manage compliance risks. Expanding existing control frameworks to include soft controls and enhanced training and communication programs monitored by data analytics will address and shape the desired behavior within their company and (future) reporting requirements simultaneously.

## 3. Compliance programs and the CSRD

The CSRD has been developed by the European Commission ('EC') to "ensure that investors and other stakeholders have access to the information they need to assess investment risks arising from climate change and other sustainability issues". [4] The Directive entered into force on 5 January 2023 and requires EU and non-EU large public interest entities with securities listed in the EU and with over 500 employee to publish sustainability statements in 2025, covering the 2024 financial year. From 1 January 2025 this also become applicable to other large entities, reporting on 2025 financial year requirements in 2026, and to small- and medium sized public interest entities from 1 January 2026, reporting on financial year 2026 requirements in 2027.[5]
The sustainability statements are part of the annual report and need to be prepared in accordance with the ESRS. These standards specify the requirements for disclosures on ESG matters and have been drafted by the European Financial Reporting Advisory Group.[6] Core elements of the draft ESRS of November 2022 include:

- ESRS G1 *Business conduct* relates to the corporate culture and business conduct policies (ESRS G1-1), how the company prevents and detects corruption or bribery (ESRS G1-3), and the confirmed incidents of undesired behavior (e.g., ABAC, undue influence) (ESRS G1-4);
- ESRS S1 *Own workforce* relates to the company's impact on its own workforce, including how compliance with the company's policies are monitored (ESRS S1-1), and how incident management, compliance monitoring (audits) and speak up mechanisms are managed in relation to the company's own workforce (ESRS S1-2; ESRS S1-3);
- ESRS S2 *Workers in the value chain* includes third party risk management ('TPRM') topics, such as, how compliance to human rights policy commitments is monitored (ESRS S2-1), and incident management, compliance monitoring (audits) and speak up mechanisms extending to the value chain (ESRS S2-2; ESRS S2-3).

The Non-Financial Reporting Directive ('NFRD') that currently applies to companiessubject to the CSRD already includes these topics. Therefore, metrics such as the number of employees (as % of total employees) following or passing a Code of Conduct training may already be measured and disclosed, irrespective of the maturity of the associated compliance program.
For the non-listed companies and small- or medium sized public interest entities, currently no specific requirements apply to report on ABAC or compliance training within an annual report. The CSRD and ESRS will therefore require more ABAC and compliance training information to be publicly disclosed for these companies. We have historically seen that the maturity of a compliance program is driven by

4. https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

5. Frikkee, M. et. al. (2023). Get ready for the Corporate Sustainability Reporting Directive. Retrieved from: https://kpmg.com/nl/en/home/topics/environmental-social-governance/corporate-sustainability-reporting-directive/get-ready-for-the-corporate-sustainability-reporting-directive.html
6. At the date of publication of this article only draft ESRSs are available and therefore the actual reporting requirements in the future could potentially differ from those described in this article.

regulatory scrutiny or obligation, of which non-listed and small- or medium sized public interest entities are usually not included. Therefore, for these companies the maturity of training programs and associated data may be limited and will require additional effort to comply with the CSRD expectations.

In addressing the CSRD, CCOs should begin with ESRS G1, which is the most relevant for the risk culture, training, and communication across the entire company. Compliance activities encompassing ESRS G1 include:

- Company values, tone at the top, Senior Management engagement; periodically assessing risk culture;
- Assessments including ABAC, Conflicts of Interest, Fraud, TPRM etc., which support the content and focus of risk-based training and communication;
- Regular and frequent communications and training, third party participation in training programs, culture / tone of compliance and regulatory change;
- Due diligence and background screenings, performance management and compensation / incentives, enforcement of disciplinary measures and accountability;
- Mission, vision, values statements, compliance policies and procedures, including the Code of Conduct, regulatory change management;
- Monitoring and tracking of regulatory changes, compliance audits and third-party reviews;
- Speak Up mechanism and protection against retaliation, responding to internal and external enquires, issues management and remediation;
- Root cause analyses, key performance and key risk indicators embedded across the company related to compliance and risk culture; and
- Internal and external reporting related to company risk culture, Board of Management diversity requirements.[7]

More specifically, ESRS G1-3 paragraph 15 requires a company to "provide information about its system to prevent and detect, investigate, and respond to allegations or incidents to corruption and bribery including the related training". The training referred to is provided to the company's own workforce and is further defined in ESRS S1 Own workforce in Appendix A as "those initiatives that the company put in place aimed at the maintenance and/or improvement of skills and knowledge". A company's own workforce includes those that are in an employment relationship with the company, self-employed workers and temporary workers provided by employment agencies. The last two groups generally have higher risk exposures than own employees and have also historically been left out of training and communication programs due to the distance from the company's responsibility. This distance has narrowed in recent years, and therefore the associated risk exposure should be managed accordingly.

The nature, scope and depth of ABAC training programs offered or required by the company must be disclosed in accordance with ESRS G1-3 paragraph 20a. This is partly qualitative information but is expected to be supported with quantitative information as well. ESRS G1.AR8 give examples of details that companies can provide, such the number of own workers that received training in the financial year and the total number of own workers, the delivery method (e.g., classroom or computer-based training), the duration (e.g., number of hours), the frequency (e.g., annually and event-driven), and the topics covered in the training (e.g., definition of corruption, Code of Conduct, Human Rights Policy, etc.).

The second disclosure requirement in ESRS G1-3 paragraph 20b constitutes a specific example of a new reporting requirement and states that the company must disclose the percentage of functions-at-risk covered by training programs. The functions-at-risk are defined in ESRS G1.AR4 and are those that are classified as such due to the increased risk to ABAC because of its tasks and responsibilities. Examples are those functions that have interactions with government officials and employees involved in procurement and sales.

ESRS G1-3 paragraph 20c is the last key disclosure requirement for compliance training, and requires information relating to members of the administrative, Supervisory and Management bodies (where applicable). The information for this group and other groups such as the functions-at-risk can be presented in a tabular format.

Each of these Compliance activities work together to manage a company's risk culture at every functional layer and location. These activities are also interdependent, meaning that a gap or strength in one area may significantly influence the maturity of the compliance program and the perception of risk culture within the company. For example, a robust compliance risk assessment and risk appetite based on strategy and objectives are the starting point for clear policies and procedures and employee screenings. This enables the development and implementation of training and communication targeted and effective per the employee's role (e.g., interaction with public officials). Monitoring the completion of targeted training and assessing the tone at the top of Senior Management via key performance indicators and employee surveys supports root cause analysis and data analytics for reporting. Creating an environment for employees to Speak Up against undesired behavior, and a mature investigations approach also supports oversight of ad-hoc incidents and enforces the desired culture within the company. Technology supports the overall effi-

7. Groen, L. et al. (2022). The state of ethics and Compliance in the Netherlands – 2022 Chief Compliance Officer Survey results. KPMG Netherlands. Retrieved from: https://kpmg.com/nl/en/home/insights/2022/02/the-state-of-ethics-and-compliance-in-the-netherlands.html

ciency and connectivity of these activities and enables reporting both internally and externally on compliance metrics, such as those included in ESRS G1. CCOs should therefore remain aware of their maturity level for each of these areas to understand where existing information is available to comply with ESRS G1, and where further work is required.

The result of the compliance maturity assessment should be used to develop the Compliance section of the integrated control framework. Control frameworks work to avoid costs, incidents, and harm associated with engaging in key compliance risks. Integrated control frameworks combine the key risk areas of a company (e.g., finance, compliance, cyber, procurement, operations, supply chain etc.) via a consistent and aligned approach. This integrated approach fosters trust in commercial transactions and enhances reputation to an acceptable level within risk appetite, while supporting efficient and effective operations. Integrated control frameworks provide an exhaustive view of processes, risks, control, and reporting requirements across each risk area. The integrated control framework is essentially a tool to implement each of the compliance program activities and foster risk culture.

## 4. CCOs must act now to identify the CSRD gaps within their compliance frameworks

In 2021 KPMG Netherlands Forensic surveyed 100 chief ethics and compliance officers to determine the state of ethics and compliance within the Netherlands. Key conclusions from this survey confirm that CCOs, and their companies, should act now to be prepared for the CSRD. Key activities to refine include doing more in the areas of ESG, integrating compliance key performance and risk indicators, utilization of data analytics, and viewing compliance training and communication as a tool to shape and assess risk culture.[8]

We often find that companies, irrespective of their size, do not have mature compliance training approaches in place to cover the requirements of ESRS G1. This includes an inaccurate or incomplete view of the training provided to their entire workforce and extending within the value chain, language considerations and blue-collar employees who may not have access to e-learnings. Companies that do have a mature approach often struggle with data quality and volume, as well as a consistent flow of information between intragroup entities for data analytics. Burdensome training in terms of length and amount, and a lack of targeted and effective compliance monitoring are also common improvement areas. A comprehensive assessment of a company's risk culture is also an area for CCOs to review for potential gaps, as only 28% of CCOs stated that they measure the success of their compliance training and communication program through employee surveys.[9]

Irrespective of the topic, data analytics will be required to comply with the CSRD reporting. Therefore, revisiting the current approach for compliance training and risk culture should include a determination of what data is required for the CSRD to prevent unavailable or incorrect data at the time of reporting. A gap analysis for the CSRD preparation and implementation will also require cross-functional collaboration for data collection and improvement. For example, data quality is often challenging, especially when a company has grown quickly or when connection of tools has not been a priority. Data collection regarding compliance training and risk culture will also involve data privacy and protection considerations, cyber and security access restrictions, and human resources information for applicability of training per role, amongst others. CCOs should therefore work alongside the Sustainability departments, Finance, and other functions to implement an integrated approach that accounts for the interconnectedness of the CSRD.

A targeted approach for risk culture perception is also advised, to further identify root causes of soft control weaknesses and determine a baseline for (future) risk culture related to the CSRD reporting. Conducting a risk culture assessment is one way to achieve this.

## 5. Conclusion

While the CSRD reporting timelines may seem far away, many companies require additional effort to become compliant in time. Implementation projects should be cross-functional due to the broad scope for the CSRD requirements. Companies give the CSRD implementation to Finance or Sustainability departments to manage. However, Compliance plays an integral role as well – especially in relation to the integrated control framework and compliance programs which help to shape the company's training, communication, and risk culture relevant to the ESRS G1, ESRS S1 and ESRS S2. Existing compliance programs and integrated control frameworks should therefore be used to support the transition to, and execution of, the CSRD reporting.

More work may be required for many companies to resolve gaps and establish their reporting baselines.

8. Groen, L. et al. (2022). The state of ethics and Compliance in the Netherlands – 2022 Chief Compliance Officer Survey results. KPMG Netherlands. Retrieved from: https://kpmg.com/nl/en/home/insights/2022/02/the-state-of-ethics-and-compliance-in-the-netherlands.html

9. Groen, L. et al. (2022). The state of ethics and Compliance in the Netherlands – 2022 Chief Compliance Officer Survey results. KPMG Netherlands. Retrieved from: https://kpmg.com/nl/en/home/insights/2022/02/the-state-of-ethics-and-compliance-in-the-netherlands.html

CCOs should begin with ESRS G1, which is the most relevant for the risk culture and training across the entire company. They can conduct a compliance maturity assessment to create a roadmap that addresses gaps while also establishing and refining data for the CSRD. A targeted assessment for risk culture is also advised to further identify root causes of soft control weaknesses and determine a baseline for risk culture. CCOs and other functions tasked with the CSRD transition should act now to prevent uncoordinated approaches and insufficient data which will ultimately fail to meet the CSRD requirements.