Building High-Quality Governance and ESRS G1 Disclosures Using OECD Due Diligence Guidance for Responsible AI

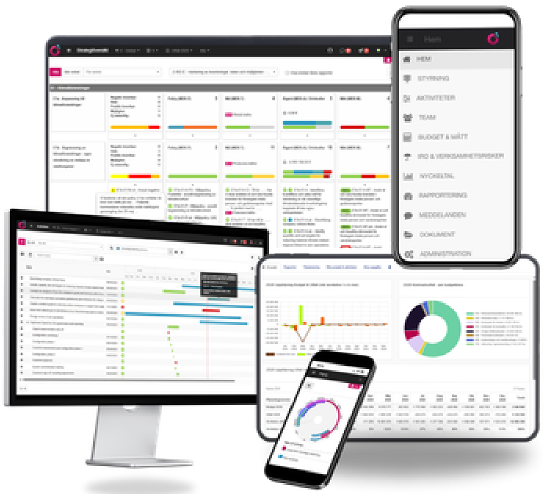
Companies are increasingly deploying AI in core operations, decision-making, and customer-facing services. As this happens, ESRS G1 Business Conduct requires them to demonstrate that their governance systems, policies, and disclosures can prevent misconduct, protect rights and ensure responsible behaviour.

To do so AI-related impacts and risks should be integrated into the relevant G1 sub-topics. If AI is related to material impacts, risks or opportunities that are not covered—or not covered with sufficient granularity—by existing ESRS topics, AI should be added as an entity-specific topic in accordance with revised ESRS 1 paragraph 11.

The OECD Due Diligence Guidance for Responsible AI provides a practical, internationally recognised framework that companies can use to build these systems.
This article translates the OECD guidance into concrete steps that companies can implement to strengthen governance and produce high-quality ESRS G1 disclosures.

The full OECD Due Diligence Guidance for Responsible AI can be downloaded here:

https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/oecd-due-diligence-guidance-for-responsible-ai_7831bb49/41671712-en.pdf



CLEERIT
A higher goal

1. Use the OECD Due Diligence Framework as the Backbone of ESRS G1 Governance

The OECD framework is built around six steps: embedding responsible conduct into management systems, identifying risks, preventing and mitigating harm, tracking performance, communicating transparently, and providing remediation. These steps map directly to ESRS G1 expectations.

The OECD framework is structured around six iterative steps :

1. Embed responsible business conduct (RBC) into policies and management systems
2. Identify and assess actual and potential negative (adverse) impacts
3. Cease, prevent, and mitigate negative impacts
4. Track implementation and results
5. Communicate actions to address impacts
6. Provide for or cooperate in remediation

These steps map naturally to ESRS G1 requirements for:

- governance structures
- policies and codes of conduct
- risk management
- whistleblowing and grievance mechanisms
- anti-corruption controls
- transparency and accountability

Companies should therefore treat the OECD framework not as an abstract model but as a practical workflow for building and demonstrating responsible business conduct.

2. Build Governance Structures That Can Actually Manage AI Risks and Negative Impacts

Governance begins with clarity. Companies must define who is responsible for AI oversight, how decisions are made, and how accountability is enforced. The OECD guidance stresses that senior leadership must own AI due diligence. For ESRS G1, this means establishing a board-level mandate for responsible AI and integrating AI oversight into existing committees rather than creating isolated structures.

Operational teams—legal, compliance, IT, HR, procurement, risk—must understand their roles. AI governance cannot sit in a single department.

Companies should document responsibilities for model development, procurement, deployment, monitoring, and incident response. This documentation becomes part of ESRS G1 disclosures and demonstrates that governance is not theoretical but operational.

Embedding responsible business conduct into existing management systems is essential. Companies should integrate AI considerations into risk management, procurement, product development, service implementation, HR policies and compliance processes.

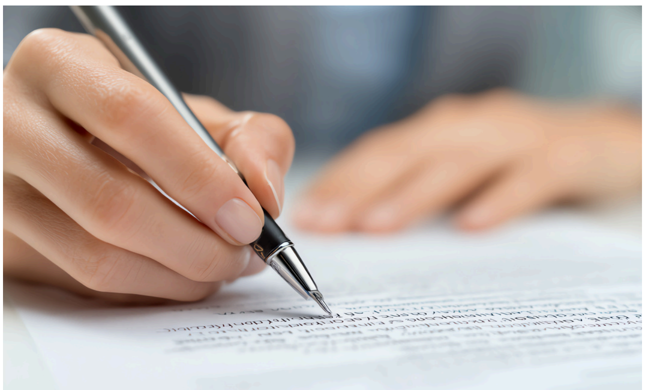
The OECD guidance emphasises that responsible AI is not a separate track; it must be woven into the organisation's existing governance fabric.

3. Develop Policies That Set Clear Expectations for Behaviour and Decision-Making

Policies are the foundation of responsible conduct. The OECD guidance stresses that companies must articulate clear commitments and behavioural expectations. For ESRS G1, this means adopting a Responsible AI Policy that sets out principles such as fairness, transparency, robustness, human oversight, and respect for rights. The policy should be practical enough for operational teams to apply and broad enough to cover evolving technologies.

Existing business conduct policies must also be updated to reflect AI-related risks. Anti-corruption policies should address automated decision-making and algorithmic scoring. Whistleblower policies should explicitly cover AI-related concerns. Human rights policies should include risks linked to data collection, model bias, and downstream impacts. Supplier codes of conduct should require responsible AI practices across the value chain.

Policies must be accessible, regularly updated and supported by training.



4. Identify and Assess AI-Related Impacts and Risks in a Structured and Repeatable Way

Risk identification is central to both OECD due diligence and ESRS G1. Companies must assess risks (for the company) and negative impacts (on people and on the environment) across the entire AI lifecycle—from design and data collection to deployment and operation.

This requires structured processes, not ad-hoc reviews.

The OECD guidance highlights several categories of risk and negative impacts: discrimination, privacy violations, worker harm, misinformation, cybersecurity vulnerabilities, environmental impacts, labour exploitation in data annotation, and dual-use concerns. Companies should evaluate how each category applies to their systems and contexts.

Prioritisation is essential. The OECD recommends assessing risks and impacts based on severity and likelihood, with particular attention to negative impacts on vulnerable stakeholders.

Companies should define risk/impact-tolerance thresholds and document how they decide which impacts and risks are material.

This documentation becomes part of ESRS G1 disclosures and demonstrates that risk and IRO management is systematic rather than superficial.

5. Implement Measures That Prevent and Mitigate Harm in Practice

Once negative impacts and risks are identified, companies must implement measures to prevent and mitigate harm. The OECD guidance provides concrete examples that companies can adopt.

Technical safeguards include bias detection tools, data governance controls, explainability mechanisms, traceability systems, and content provenance tools. Organisational safeguards include human oversight protocols, safe deployment procedures, and clear escalation paths for high-risk decisions.

Before deployment, companies should conduct scenario planning, test systems in realistic environments, and stress-test for misuse. They should establish “go/no-go” criteria that determine whether a system is safe to release.

During operation, companies must monitor model performance, detect drift, update models responsibly, and suspend or decommission systems that become unsafe.

ESRS G1 disclosures should describe these controls and demonstrate that they are applied consistently.

6. Monitor, Audit, and Document AI Governance Continuously

The OECD guidance emphasises continuous monitoring. Companies should track incidents, complaints, model performance, bias metrics, security events, and supplier compliance. Monitoring must be systematic and documented.

Audits—internal and external—should evaluate the effectiveness of controls, the integrity of data, the robustness of models, and the adequacy of governance structures. Companies should audit AI systems used in compliance, procurement and financial processes, as these systems can directly influence business conduct.

Record-keeping is essential. Companies must maintain detailed documentation of risk decisions, audit trails, model changes, and incident responses.

This documentation supports ESRS G1 disclosures and **demonstrates traceability** across the AI lifecycle.

7. Communicate Transparently and Produce High-Quality ESRS G1 Disclosures

Transparency is a core OECD expectation and a central ESRS G1 requirement. Companies must communicate their governance structures, policies, risk assessments, mitigation measures, monitoring systems, incidents, remediation actions, and supplier governance.

High-quality disclosures are clear, specific, balanced, evidence-based, and accessible. They avoid generic statements and provide concrete examples. They acknowledge limitations and describe improvements.

Transparency builds trust and reduces regulatory friction.

8. Provide Remediation and Operate Effective Grievance Mechanisms

The OECD guidance dedicates an entire step to remediation. Companies must provide channels for reporting concerns, including AI-related issues such as discrimination, harmful automated decisions, privacy violations, misuse, unsafe deployment, and labour exploitation in data supply chains.

Grievance mechanisms must be legitimate, accessible, predictable, equitable, transparent, and rights-respecting.

Companies must protect whistleblowers and ensure that complaints lead to meaningful remediation.

ESRS G1 disclosures should describe how complaints are handled, how remediation is provided, and how lessons learned lead to improvements.

9. Engage Stakeholders Throughout the AI Lifecycle

Stakeholder engagement is one of the strongest themes in the OECD guidance. Companies should engage workers, unions, affected communities, customers, civil society, experts, and SMEs throughout the AI lifecycle—from design and data collection to deployment and post-deployment evaluation.

Engagement improves product quality, reduces risk, strengthens governance, and supports regulatory compliance.

ESRS 2 SBM-2 requires companies to disclose how they engage stakeholders and how this engagement influences decisions.

10. Use This Framework to Build Practical ESRS G1 Governance

You can use this article and the OECD Due Diligence Guidance for Responsible AI as a practical guide to build governance systems that meet ESRS G1 expectations.

It provides a blueprint for policies, risk and impact management, controls, monitoring, remediation, stakeholder engagement, and disclosures.

It can be used for training, policy drafting, risk and impact assessments, supplier governance and reporting.

By progressing in a structured and deliberate manner, your organisation will strengthen its command of AI-related issues and consolidate exemplary governance that is fully aligned with European expectations.

Disclaimer

The content of this publication reflects CLEERIT's current understanding. This information does not replace information provided by official, administrative, or governing authorities. The information contained in this publication is subject to change, correction, or addition without notice. While every effort has been made to ensure that the information contained in this publication is accurate and complete, inaccuracies may exist. CLEERIT accepts no liability for any loss or damage that may arise in connection with the use of the information contained in this publication.

CLEERIT

A higher goal