GAN INTEGRITY

Guide

CSDDD

Everything you need to know about the CSDDD and how you can start preparing for it

What's inside

Contents

Introduction

Earlier this year, the European Union finalized the Corporate Sustainability Due Diligence Directive (CSDDD) draft proposal stirring up significant debate among corporations and EU member states around the stringency of the requirements on organizations in scope. Following amendments to the Directive, it was approved by the European Parliament on April 24th, 2024 and formally approved by the European Council a month later marking a significant step towards the enforcement of new environmental and human rights standards. This far-reaching legislation will bring about fundamental changes in supply chain management for both EU and non-EU companies as the European Commission leans on legislative tools to promote human rights and environmental sustainability.

At face value, the requirements imposed by the Directive may appear daunting for already time and resource-constrained compliance teams. Identifying and mitigating risks across chains of activity could potentially involve hundreds and thousands of supplier relationships. However, companies can proactively stay ahead by establishing scalable processes to enable proportionate and efficient risk management and compliance with the Directive.

This guide will break down the requirements of the Directive and address how companies can start preparing for it already today.

Who is subject to the Directive

The CSDDD applies to a wide range of entities, including EU and non-EU companies, categorized into distinct groups based on criteria such as size and turnover leveling the playing field, while protecting the environment and promoting sustainable investment. The Directive will apply to the following groups of companies;

EU Companies

Group 1: Companies with;

1. more than 5000 employees or more on average;
2. more than EUR 1.5B in net turnover worldwide within the past financial year.
3. Companies that do not fall into this group, but are the ultimate parent company of a group reaching these thresholds are also liable under the Directive.

Group 2: Companies with;

1. 3,000 employees or more on average;
2. more than a net worldwide turnover of EUR 900 million within the past financial year.

Group 3: Companies with;

1. 1,000 or more employees on average
2. a net worldwide turnover of more than EU 450M within the past financial year.

Group 4: Companies with franchising or licensing agreements within the EU that, within the past financial year have;

1. Generated a net turnover of more than EUR 22.5 million;
2. Generated individually or, on a consolidated basis — as the ultimate parent company of a group of companies - an aggregate worldwide turnover of more than EUR 80 million.

Non-EU Companies

Group 1: Companies with;

1. more than EUR 1.5B in net turnover in the EU within the year preceding the last financial year.
2. Companies that do not fall into this group, but are the ultimate parent company of a group reaching these thresholds are also liable under the Directive.

Group 2: Companies with;

1. more than EUR 900M in net turnover within the European Union in the year preceding the last financial year.

Group 3: Companies with;

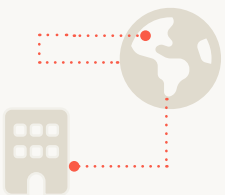
1. a net turnover of EUR 450M or more within the European Union in the year preceding the last financial year.

Group 4: Companies with franchising or licensing agreements within the EU that, within the year preceding the last financial year;

1. Generated a net turnover of more than EUR 22.5 million;
2. Generated individually or, on a consolidated basis — as the ultimate parent company of a group of companies - an aggregate worldwide turnover of more than EUR 80 million.

Representation of third-country companies:

In-scope third-country companies must designate an authorized representative that is mandated by the company to act on its behalf in compliance with the CSDDD. Authorized representatives must be located within the EU member state in which the third-country company operates.



Implementation timeline of the Directive:

- **2027:** Three years after the enforcement of the Directive Group I will be expected to be compliant with its requirements
- **2028:** Companies in Group II are granted an additional year before they are held accountable to the Directive's requirements.
- **2029:** Companies in Group III and IV will be granted a five-year timeline within which they will need to become compliant with the Directive.

Transposition of the Directive and enforcement supervision:

Once transposed, each member state will allocate a supervisory body to oversee the implementation and compliance with the Directive within their respective jurisdictions. Member States have jurisdiction over EU companies registered within their borders, as well as non-EU firms with a branch in or that generate most of their EU turnover within their respective territories. Representatives of each national body will collectively make up a European Network of Supervisory Authorities to facilitate cooperation and coordination between national authorities.

Penalties for non-compliance:

Failure to comply with the CSDDD can lead to monetary penalties, with the maximum fine being no less than 5% of the company's net worldwide turnover.

Preparing for compliance with the CSDDD

The Directive outlines a set of requirements for accountable companies, these include;

- Embedding due diligence practices into organizational policies and risk management systems to ensure comprehensive coverage of sustainability considerations.
- Conducting thorough assessments to identify potential or actual adverse impacts within the company's operations, subsidiaries, and related chain of activity involving business partners.
- Collaboration with stakeholders to develop an action plan with clearly defined timelines aimed at preventing and/or mitigating potential impacts effectively.
- Immediate or gradual measures to minimize impacts where instant cessation is not feasible.
- Qualitative and quantitative indicators to measure progress, track improvement, and evaluate the effectiveness of mitigation efforts.
- A transition plan for climate change mitigation.
- Establishment and maintenance of a notification mechanism and complaints procedure
- Transparent and public communication on the organization's due diligence efforts.

Defining the chain of activity:

The term "chain of activities" refers to the sequence of activities performed by a company's business partners upstream and downstream. Upstream activities encompass tasks like design, extraction, sourcing, manufacturing, transport, storage, and supply of raw materials, products, or parts used in the company's goods or services. Downstream activities involve the distribution, transport, and storage of the company's products by business partners acting on behalf of the company, excluding export-controlled products. However, for regulated financial entities, only upstream activities are covered, excluding downstream partners that receive services or products from the company.

Leveraging the OECD due diligence guidelines framework

Aligned with international standards such as the UN's guiding principles on business and human rights, the OECD guidelines for multinational enterprises, and the OECD due diligence guidance for responsible business conduct, companies can benefit from a hands-on step-by-step guidance on how to approach due diligence. These include the following areas;

Integrating responsible business conduct into policies and management systems

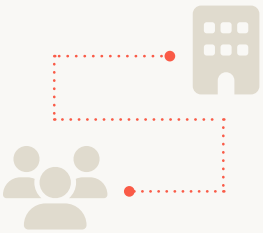
Devising the right policies for the organization's employees and third parties is critical, ones that serve as guiding principles for how the company expects anyone working on its behalf to carry out business. This pillar of the OECD guideline emphasizes not only the availability of these policies to all stakeholders but also their seamless integration into the company's day-to-day operations.

Identifying and assessing actual and potential adverse impacts

Companies are required to identify risks inherent within their chain of activities, spanning sectors, products, geographies, and enterprises. This entails a comprehensive assessment of the company's ability to access relevant information, addressing any gaps in data availability. Moreover, the risk identification process must encompass an analysis of both upstream and downstream activities to discern potential adverse impacts originating from the company's operations, its subsidiaries, and business partners.

In prioritizing relationships for vetting, companies should focus on the risk profile of each partner rather than the strength of the relationship with the organization. Factors such as the operational location, production processes, and past assessment findings should guide this prioritization. Furthermore, companies must evaluate relationships with non-contracted entities like sub-suppliers or subcontractors. Assessments can be conducted through various means, including information disclosure requests, certifications, and collaborative initiatives, ensuring a thorough understanding of risk exposure across the supply chain.

Seeking assurances from business partners and their respective suppliers



The Directive explicitly establishes the necessity to seek contractual assurances from an organization's direct business partners as well as the latter's respective contributors to the organization's chain of activities — these may include sub-suppliers, subcontractors, etc. — that commit all actors to the adherence with the client organizations' code of conduct and measures imposed by the organization's action plan, including verifications of compliance.

Ceasing, preventing, and mitigating adverse impacts

Once risks have been identified and assessed, companies must implement an action plan to prevent and mitigate any adverse impacts. The guidelines delineate between various approaches, including concrete steps to adapt company operations, products, and services to avert adverse impacts. Proactive measures such as employee and partner training, policy development, and other interventions are vital for preventing adverse outcomes.

How companies choose to address adverse impacts may vary depending on their causation. For impacts directly caused by the company, remedial action is necessary, potentially involving ceasing or preventing the impact altogether, even if it entails disengaging from the business partner. Conversely, impacts contributed to by business relationships necessitate leveraging the company's influence to mitigate the impact. Prioritizing actions based on the immediacy and severity of risks is crucial to effectively managing adverse impacts as or before they unfold.

Responsibility to support SMEs within the supply chain to enable the effective implementation of action plans

Organizations subject to the Directive have an obligation to provide 'targeted and proportionate support' for SEMs with whom they have an established business relationship. This enables compliance of SMEs with the company's policies and adequate implementation of mitigation measures.

Tracking of implementation and results

Companies must effectively track implementation of measures and related results and will therefore need to establish measurable metrics. These can be quantitative or qualitative based on the nature of the actions. Tracking should be periodic, with the ability to continuously monitor how changes may impact measures such as alterations in operations, business pivots, or other. In the same way relationships and risks were prioritized for assessment and mitigation, tracking and monitoring should also be prioritized based on the significance of the potential or actual adverse impacts.

Communicating how impacts are addressed

Companies will need to communicate externally to all relevant stakeholders on policies and due diligence processes and the measures put in place to prevent or mitigate adverse impacts. Communication channels should be accessible and tailored to the audience, accommodating various forms to ensure clarity and understanding. The OECD guidelines take into account cases where information is commercially sensitive or poses other competitive or security concerns and provide guidance on how companies can approach disclosing information in these cases.

Providing for or cooperating in remediation when appropriate

The OECD guidelines delineate between various forms of remediation depending on the availability of domestic and international standards and the preference of impacted stakeholders. Establishing a grievance channel, such as a hotline or an incident reporting portal, enables companies to gather input and feedback on the efficacy of their mitigation efforts. Additionally, these channels serve as avenues for surfacing risks that may not have been previously identified or assessed as severe by the organization.

Intake channels also empower organizations to adopt a proactive stance toward early risk identification, facilitating timely intervention before adverse impacts escalate in severity. By leveraging these mechanisms, companies can not only address existing issues promptly but also preemptively mitigate potential risks, bolstering their commitment to responsible business practices and stakeholder engagement.

Collaboration and sharing among peer groups

The Directive underlines collaboration with others as a strong enablement tool to increase companies' ability to bring the adverse impact to an end.

How you can start preparing for the Directive

Regardless of how the Directive will be transposed, companies are under mounting pressure to adopt more sustainable practices and enforce higher sustainability standards throughout their third party and supply chain ecosystem. This trend is fueled by increasingly informed consumers who prioritize products and services with minimal human and environmental impacts, driving a shift toward more conscious purchasing decisions. The same is true for investors; who now place greater emphasis on effective management and mitigation of Environmental, Social, and Governance (ESG) risks.

Preparing your organization for forthcoming, stricter sustainability regulations is not only prudent but also strategically advantageous. But where should you begin?

Train and raise awareness

There is no doubt that the CSDDD stands out for its extensive reach in supply chain vetting and risk mitigation, surpassing other due diligence regulations: The CSDDD mandates a comprehensive assessment and mitigation strategy across the entirety of a company's chain of activity, rather than confining scrutiny to the initial tiers. This will impact many teams within your organization to varying levels.

To effectively navigate these requirements, it is essential to understand how each team can help identify, assess, mitigate or even prevent actual or potential adverse impacts in the company's operations. This will require educating the workforce by raising awareness of potential policy changes, updated codes of conduct, accompanied by relevant training. Training your workforce will also better enable them to identify and flag potential or actual failures or adverse impacts back to your organization.

Understanding where to focus through risk mapping

If your company falls within the purview of the CSDDD, chances are you operate a vast, global, and intricate supply chain ecosystem. Fortunately, the risk mapping and assessment requirements outlined in the Directive do not prescribe a one-size-fits-all approach to every business partner and supplier. Instead, it advocates for a proportional strategy, aligning with the principles outlined in the OECD due diligence guidelines. This allows you to concentrate your efforts where they are needed the most.

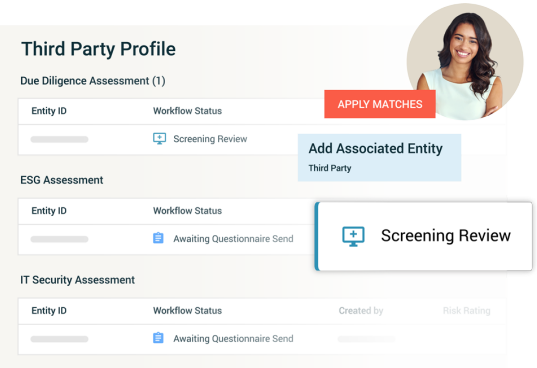
Once you've mapped out your supply chain, the next step is to pinpoint where potential risks lie and assess their severity. Technology can be invaluable in this process, enabling the automation of data collection and assessment, and streamlining procedures across the organization.

When building a business partner risk profile through the collection of different sets of information (such as questionnaires, internal business justification forms, enhanced due diligence reports, data screening reports, etc.) technology can help you parse through the data, aggregate the findings, and apply business rules to assess the level of risk. The initial assessment can automate low-value work by filtering out all relationships that don't need any human intervention while automatically approving and logging these with an auditable trail of activity available for reference. Medium and high-risk partners can be escalated based on a set of pre-defined rules, for further review with the right stakeholders.

By harnessing technology to sift through the complexities of your supplier population, you not only make risk management more manageable but also establish a structured approach to risk identification and relationship prioritization.

Involve stakeholders and govern access and engagement in the due diligence process

The Directive explicitly references 'consultation with stakeholders' when it comes to the development and implementation of a company's action plan. But engaging stakeholders can be tricky, particularly with teams less directly involved in regulatory compliance, where such tasks may be viewed as hindrances to business operations. But it doesn't have to be. Make sure to involve stakeholders across the business early on in the process. As policies are revised and new procedures are developed, reaching out to counterparts, asking questions, and demonstrating genuine curiosity about their processes can create a sense of inclusion among stakeholders. This involvement fosters a feeling of ownership and responsibility, encouraging proactive engagement and accountability for the effectiveness of actions.



With potentially multiple risk types needing individual subject-matter expert assessments comes the risk of process bottlenecks and business disruption. To address this challenge, technology can help streamline stakeholder engagement through a non-linear process. This allows for the progression of multiple assessment flows simultaneously speeding up turnaround on the overall assessment of relationships.

The same applies to stakeholders across other business departments, from procurement to finance, sales, and others, a role-based access control infrastructure built into your program enables cross-team collaboration on business relationships simultaneously. Governing access to only the data each user needs to action or assess will ensure that the right people are pulled into the right process at the right time.

Consider your suppliers' experience and enhance it

Have you ever seen your business partners get excited about information collection? Disclosure requirements are only getting more stringent under the CSDDD but the reality is that, even with regulatory obligations, dealing with information gaps won't go away. Completeness of information is still a challenge for effective risk identification and assessment. But to alleviate the burden, make sure you carefully consider the experience your are offering your company suppliers. Making the process less burdensome can go a long way in collecting the data you need.

Information disclosure can be made easy when you consider the experience of your business partners. How burdensome is the process you're putting them through? Is the experience tailored to the nature of their business, operations, geography, etc.? Are you sending your suppliers lengthy Word documents or enabling them with intuitive platforms and tailored low-touch user journeys? User-focused applications can go a long way to guide your suppliers through tasks, increase adoption, and provide you with a higher rate of data completeness and accuracy.

Develop an action plan that is tightly related to your risk mapping

Every evaluation and risk identification should be followed by appropriate mitigation and prevention measures. The identified risk levels and severity of adverse impact should inform the measures that need to be taken. Risks exceeding your business' risk tolerance should lead to a termination or rejection of the business relationship. Where risk can be managed through mitigations, appropriate measures should be attached to immediate next steps.

Measure effectiveness, monitor changes, and act on events in real-time

Implementing a centralized system to oversee all supplier-related information and action plans is essential to effectively manage performance. Fragmented data and isolated processes with dispersed ownership can impede the ability to gauge the effectiveness of measures.

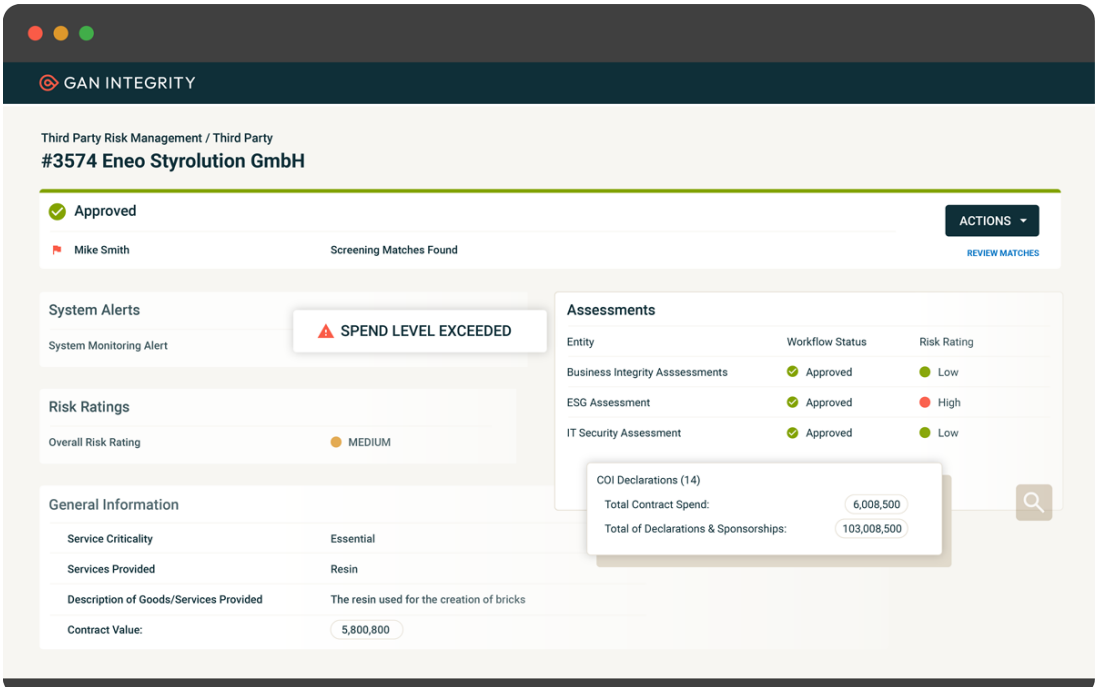
A centralized system provides comprehensive visibility into all supplier relationships, offering a holistic view of program progress. At the individual relationship level, centralization is equally vital, enabling focused examination of high-risk suppliers by aggregating relevant data, due diligence activities, and associated mitigation efforts.

You can't measure what you can't manage. Consolidating data in one location will therefore make it easy to report and measure effectiveness, saving valuable time. It will also allow you to more efficiently spot bottlenecks to implementation and address these as needed.

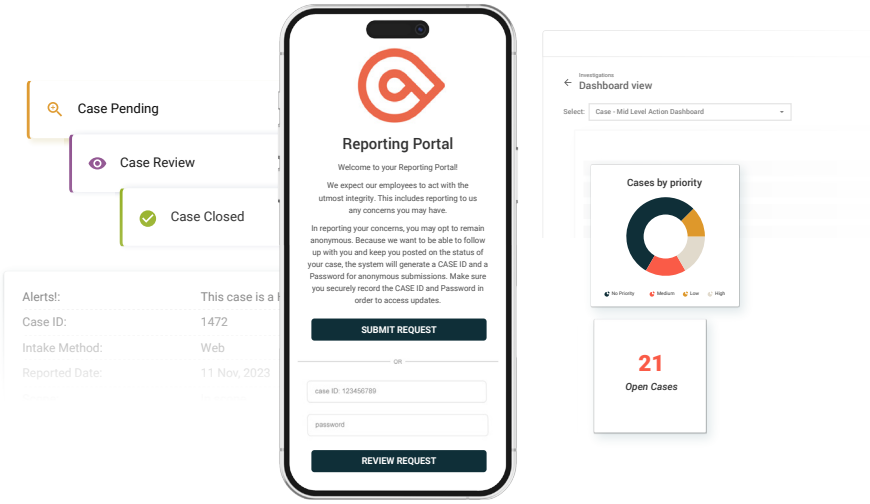
Flowing data in a structured way back into a centralized system will also enable stakeholders to monitor changes in real time. The Directive stipulates the need to periodically review relationships throughout their lifecycle; a task that can be easily automated. However, changes that impact underlying risk indicators wouldn't be visible if no capabilities of dynamically monitoring these changes are built into your program. Consider these factors when assessing the technology that underpins available monitoring capabilities to ensure that you stay on top of changes that impact the adequacy of your measures.

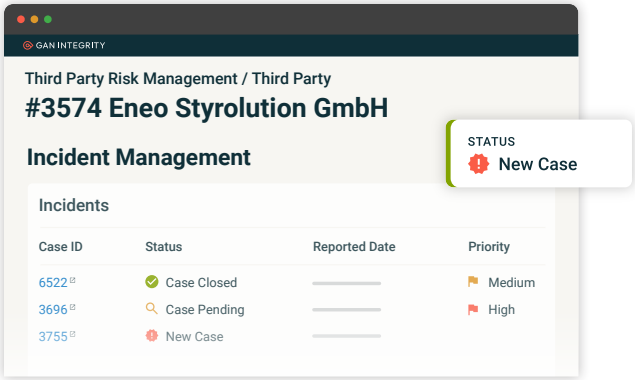
Set up a grievance mechanism and connect it to your due diligence program

The CSDDD mandates setting up a complaints procedure allowing anyone within the chain of activity to voice concerns. Similar to optimizing the disclosure experience for suppliers, incident reporting also demands careful consideration. Making it easy and accessible to reporters is the first consideration. Think of which tools you are putting at their disposal: Are these accessible and usable? Are they easy to interact with and can reporters follow up on resolutions?



Beyond the aforementioned, consider how you can make a grievance channel accessible to all and use the insights to spot risks you may not have identified during your assessments. Connecting data from your due diligence processes to your incident management program can give you an advantage. Integrated technology can help you create connections between data where relevant. Business relationships that are subject to reports or investigations can be flagged on your risk profiles ensuring that the owner of those relationships has a full view of potential failures. This not only brings all stakeholders into the loop, ensuring visibility and collaboration but encourages a proactive approach that enables you and your business to address risks before they snowball into potentially unmanageable situations.





Make documentation easy

Reporting to external stakeholders on your efforts is a pillar of the CSDDD. Centralizing your program activities, action plans, adaptations, and other efforts - as described above - is therefore also relevant for reporting. Disparate systems and siloed data will make it hard and time-consuming for compliance teams to report.

Integrating your due diligence and incident management processes is also a case in point from a reporting perspective, as data can be aggregated to see which relationships are connected to investigations, how these cases are resolved, the impact it has on mitigating measures, or potentially the termination of relationships. All valuable insights to see holistically.

Conclusion

There is no doubt that the CSDDD brings encompassing requirements into play for businesses globally, however, the proposal serves as yet another reminder that companies have to consider their impact and footprint holistically. That necessitates a company-wide pivot in the way it operates, bridging gaps in process, data management, and stakeholder collaboration to ensure that growth does not come at the expense of environmental integrity and human rights. The future is about bringing business prosperity in lockstep with the prosperity of nations, their populations, and the planet. While this transformative shift may not happen overnight, with a timeline spanning two to three years, the journey toward preparation can begin today.

GAN INTEGRITY

GAN Integrity empowers companies across industries and economic sectors to take charge of their compliance program with the Integrity Platform; a no-code compliance, ethics and risk management platform that spans across multiple compliance applications; from Risk Management to Disclosures, Incident Management, Third Party Risk Management and more. Every application built on the Integrity Platform can be tailored to accommodate organizations' unique process flows and company set up. With the platform's no-code architecture, organizations can design bespoke applications to automate compliance areas unique to their business and ensure that every control is effectively run and monitored on one centralized platform.

Elevating business ethics everywhere.

Seadrill · DANONE NORTH AMERICA · CLARIOS · BARRICK · infront

Visit us at ganintegrity.com or

contact us to learn more