HREDD Performance in German Business

RISK ANALYSIS

An empirical study of §5 LkSG risk analysis and Guiding Principles 17–18 across 254 German companies.

FRAMEWORK	SAMPLE	CODED
§5, §9 LkSG	254 companies · 16 sectors	30 practices
UNGP GP 17–18	2023/2024 reporting year	4 effectiveness indicators

Global Compact Network Germany

CONTENTS

EXECUTIVE SUMMARY

Across the 254 companies in the sample, the **foundational requirements of §5 risk analysis have been established in virtually all cases**. Risk owners are formally assigned by a large majority of companies, 99.2% have conducted a risk analysis, 98.8% do so annually, and virtually all companies cover both their own operations and direct suppliers (99.2% each). The basic structure of risk analysis is broadly in place.

The **gaps emerge in depth, scope, and feedback loops**. Indirect supplier coverage drops sharply from the direct supplier baseline, despite the LkSG's §9 obligation to conduct risk analysis when concrete indications of indirect-supplier violations emerge. The majority of companies consult neither external stakeholders nor the potentially affected persons most exposed to the risks being assessed. Effectiveness tracking is the weakest dimension: few companies close the feedback loop between what the risk analysis finds and whether their response to it works. These gaps are not separate shortfalls. The practices the field has adopted least are the same ones that most distinguish the companies that validate their risk predictions, which makes participation the part of risk analysis most closely tied to whether it works.

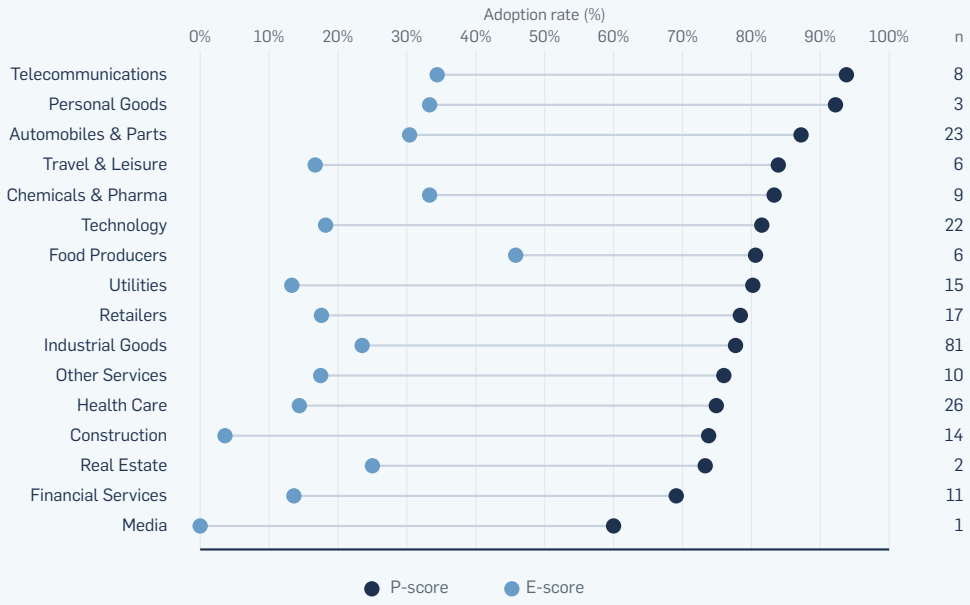
Key Findings

- **Governance infrastructure is in place; substantive analysis is not.** Stakeholder consultation (50.4%), affected-persons input (47.2%), and indirect supplier coverage (42.9%) all sit below the 75% field-standard threshold, and effectiveness tracking averages 21.0%.
- **Supply chain due diligence coverage drops sharply beyond direct suppliers – by design, but that design follows the contractual tier rather than upstream tiers where the most serious risks to affected persons often concentrate.** Indirect supplier coverage sits at 42.9% against direct-supplier coverage of 99.2%, a 56-point gap. The CSDDD's risk-based approach, as adopted under the Omnibus I amendments, contemplates indirect-supplier coverage calibrated to risk rather than contractual tier – a shift in the architecture of due diligence for which this sample's current tier-based structure is not yet configured.
- **The people most exposed to risk are largely absent from the process of identifying it.** The majority of risk analyses are conducted without external stakeholder consultation and without direct input from potentially affected persons.
- **Companies are better at evaluating risk than at finding the right risks in the first place.** Evaluation practices (severity, likelihood, prioritisation) average 90.9% adoption; scope and participation practices average below 50%. The frameworks are sophisticated; the information feeding them is not always equally comprehensive.
- **The systems rarely learn from their own findings.** Effectiveness tracking – violation recurrence, audit finding severity trends, risk prediction validation – sits below 35% uptake across all four indicators.
- **Participation is the line between a risk analysis that works and one that does not.** The practices that bring workers, affected persons, and the wider value chain into the assessment are the ones that most strongly predict whether a company validates its risk predictions: those that consult worker representatives do so at 58.3%, against 4.3% for those that do not. The widest gap in the domain is also the one most closely tied to whether the analysis works.

SECTOR AND SIZE OBSERVATIONS

Figure 1 maps **risk analysis performance across the sixteen aggregated sectors**. Each sector is shown as two connected dots: the dark dot marks its mean P-score across the 30 risk analysis practices; the light dot marks its mean E-score across the four effectiveness indicators. The horizontal distance between the two dots is the P/E gap for that sector – a structural feature reproduced across every sector in the sample.

FIGURE 1: Sector Performance – Risk Analysis P-score vs E-score



Each row represents one sector. Horizontal position shows adoption rate (%); blue dot = mean P-score (across 30 risk analysis practices P024–P053); light dot = mean E-score (across the four risk analysis effectiveness indicators (E003, E005, E016, E020). P-score range across sectors: 60-94 %; E-score range: 4-48 %. Source: LkSG disclosure analysis, n=254 companies. Sectors shown using the 16-sector aggregation (see appendix for mapping from 25 raw industries). n = number of companies per sector.

The sectors with the highest risk analysis practice adoption are Telecommunications (94%), Personal Goods (92%), Automobiles & Parts (87%), and Travel & Leisure (84%), **consistent with sustained regulatory exposure and stakeholder pressure across these sectors.**

Size effect: **practice adoption rises with company size.** Mean P-score increases from 77.7% in the 3,000-10,000 band (n=154) to 80.8% in the 10,000-50,000 band (n=72) and 86.2% among companies with more than 50,000 employees (n=28). The gap is most pronounced on the scope and participation practices where the field as a whole is weakest – indirect supplier coverage, event-driven re-analysis, and affected-persons input – all of which rise steeply from the smallest to the largest size band (see section VI)

Size effect: **practice adoption rises with company size**. Mean P-score increases from 77.7% in the 1K–10K band (n=154) to 80.8% in the 10K–50K band (n=72) and 86.2% among companies with more than 50,000 employees (n=28). The gap is most pronounced on the scope and participation practices where the field as a whole is weakest – indirect supplier coverage, event-driven re-analysis, and affected-persons input – all of which nearly double from the smallest to the largest size band.

CRITICAL GAPS

The **critical gaps in this domain concentrate in two structural areas. Scope and participation**: 145 companies (57.1%) do not extend their risk analysis to indirect suppliers (P029: 42.9%), 156 (61.4%) do not conduct event-driven analyses when circumstances warrant (P026: 38.6%), and 135 (53.1%) do not take a value-chain perspective (P030: 46.9%). **Participation shows the same shortfall:** 126 companies (49.6%) consult no external stakeholders (P041: 50.4%), 139 (54.7%) do not seek input from worker representatives (P042: 45.3%), and 134 (52.8%) collect no input from potentially affected persons (P044: 47.2%).

Effectiveness tracking: all four indicators sit below threshold – violation recurrence (E003: 10.6%), audit finding severity (E016: 10.2%), risk prediction validation (E005: 28.7%), and supply chain traceability (E020: 34.6%). The 58-point gap between the sample average P-score (79.1%) and E-score (21.0%) is the most acute manifestation of the structural pattern: **companies have established the procedural architecture of risk analysis but not the feedback mechanisms that would allow the analysis to improve over time**.

The 75% adoption threshold marks the level below which a practice cannot be considered field-standard across the sample. Derivation and sensitivity analysis are documented in Appendix 1, with full treatment in the HREDD Research Design & Methods paper.

IMPLICATIONS FOR RIGHTS-HOLDERS

The scope and participation gaps documented here are not distributed randomly: they are most likely to **occur precisely where risks are most severe and rights-holders most vulnerable**. When risk analyses exclude indirect supply chains, bypass external stakeholder consultation, and produce no feedback on their own accuracy, the resulting picture understates harm where it concentrates – in upstream tiers, in geographies with weak labour governance, among migrant and informal workers. Rights-holders in those contexts are largely assessed ata a distance. The full implications are set out in section VII.

I. NORMATIVE FRAMEWORK

This section frames §5 and §9 LkSG and UN Guiding Principles 17–18 as the normative anchors against which the 30 risk analysis practices and four effectiveness indicators are coded.

A. UNGP Framework

This report assesses company performance against the UN Guiding Principles on Business and Human Rights (UNGPs, 2011) – specifically the **corporate responsibility to identify and assess human rights impacts under the second pillar.** The practices and indicators in this domain correspond to:

GP 17 (identifying and assessing impacts through meaningful stakeholder consultation), GP 18 (drawing on internal and external expertise, with particular attention to vulnerable groups), and GP 20 (monitoring effectiveness of due diligence) together provide the normative foundation for the practices and indicators in this domain.

The UNGPs' concept of salience – the principle that companies should prioritise the most severe potential impacts on people, rather than those most visible or reputationally significant – underpins this report's reading of risk analysis quality. Practices that incorporate severity and likelihood assessment, that draw on affected-person perspectives, and that extend analysis to where the most serious risks actually concentrate are weighted more highly than those that satisfy formal reporting requirements. This **risk-based, salience-driven approach is also the analytical framework underlying the EU Corporate Sustainability Due Diligence Directive (CSDDD).**

B. LkSG Statutory Obligations

The Lieferkettensorgfaltspflichtengesetz (LkSG) operationalises the UNGP framework in German law. Two statutory provisions are central to this report:

§5 Risikoanalyse (Risk Analysis): Companies must conduct an adequate risk analysis to identify human rights and environment-related risks in their own business area and with direct suppliers. The analysis must be conducted at least annually, and on an ad-hoc basis when circumstances warrant. It must assess the probability of violations and their severity, and enable the company to prioritise its due diligence efforts.

§9 Mittelbare Zulieferer (Indirect Suppliers): Where a company has substantiated knowledge (*substantiierte Kenntnis*) of a potential violation by an indirect supplier, it must immediately conduct a risk analysis and take appropriate preventive and remedial action. This creates an obligation of responsiveness to incoming risk signals from beyond the direct supply chain.

Obligation to make an effort *(Bemühungspflicht):* Risk analysis practices are the evidentiary foundation for demonstrating that due diligence is genuinely being conducted. The **LkSG imposes a Bemühungspflicht – an obligation to make an effort rather than an Obligation of Result (Erfolgspflicht).** Without a substantive risk analysis covering the right scope, drawing on relevant data sources, and incorporating affected-person perspectives, companies cannot show they have fulfilled this obligation.

C. EU Corporate Sustainability Due Diligence Directive (CSDDD)

The CSDDD applies across the EU from 26 July 2029 to companies with more than 5,000 employees and over €1.5 billion in net turnover, as amended by Omnibus I (2026)[1]

For risk analysis specifically, the **CSDDD departs from the LkSG in three material respects.**

1. **Scope:** where the LkSG limits mandatory risk analysis to own operations and direct suppliers (with indirect suppliers addressed only on a triggered basis under §9), the CSDDD adopts a fully risk-based approach in which the depth and breadth of analysis must follow the severity of risk, not the contractual tier.
2. **Stakeholder engagement:** the CSDDD requires meaningful engagement with affected persons and their representatives as an integral element of the risk analysis process, not a supplementary step.
3. **Effectiveness:** the CSDDD requires companies to monitor and evaluate the adequacy and effectiveness of their due diligence measures, placing the E-series indicators examined in section V at the centre of compliance rather than at its frontier.

The findings in this report therefore have direct forward-looking relevance: the critical gaps identified in scope, stakeholder participation, and effectiveness tracking are precisely the dimensions on which the CSDDD raises the bar beyond the LkSG baseline.

II. PRACTICE LANDSCAPE: RISK ANALYSIS FOUNDATIONS

§5 LkSG requires companies to conduct an adequate and effective risk analysis (angemessene und wirksame Risikoanalyse) of their own business area and direct suppliers – assessing **both the probability of violations and their severity, and prioritising action accordingly**. The proportionality principle (§3 Abs. 2 LkSG) further allows companies to calibrate required measures to their leverage, capacity, and position in the value chain – a flexibility that goes beyond the severity/likelihood weighting required under the CSDDD. The 18 practices in this section (P024–P045) capture how companies have built the foundational architecture of risk analysis: its scope, frequency, methodology, and accountability structures.

1 The CSDDD as originally adopted (2024) envisaged a phased implementation and broader scope. The Omnibus I package (European Commission, February 2026) narrowed the scope, removed the phased rollout, and modified civil liability provisions. The regulatory framework remains subject to finalisation by Member States. References to CSDDD in this report reflect the post-Omnibus I position as of April 2026.

A. Scope & Frequency – P024–P030

PRACTICE **P024**

Risk Analysis Conducted

ADOPTION RATE

99.2% (252/254)

UNGP **GP 17–18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Company conducts a systematic risk analysis to identify and assess human rights and environmental risks across its operations and supply chain.

WHY THIS MATTERS

Companies cannot prevent what they have not identified, and cannot allocate resources proportionately across a value chain they have not examined. The risk analysis is therefore the starting point for everything that follows in the due diligence cycle. Adoption is near-universal at 99.2% (252/254).

GOOD PRACTICE EXAMPLE

EDAG Engineering GmbH conducts a highly structured, multi-dimensional risk analysis using a specialised software system to generate a comprehensive risk score for each supplier and its own business area. The analysis combines five distinct data pillars: country-level risks from public indices, commodity and industry risks from historical incident data, AI-supported web and social media screening for real-time alerts, direct supplier self-assessments, and internal company insights – producing what the company terms a "360-degree risk score" for each supplier.

"[We use] country-level risks based on public indices, commodity/industry risks leveraging historical incident data, continuous AI-supported web and social media screening for real-time risk alerts, direct supplier self-assessments, and internal company insights."

PRACTICE **P025**

Risk Analysis – Annual

ADOPTION RATE

98.8% (251/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 4**	CSDDD **Art. 8**

DEFINITION

Company conducts its risk analysis at least annually, so the assessment reflects current conditions rather than a static point-in-time snapshot.

WHY THIS MATTERS

Supply chains shift. A risk analysis conducted once and never revisited is navigating present conditions with an outdated map. Stronger practice decouples the analysis from the reporting cycle so findings inform current-period preventive measures rather than documenting what was identified in the year being reported. Adoption is near-universal at 98.8% (251/254).

GOOD PRACTICE EXAMPLE

TenneT TSO GmbH exceeds the minimum requirement of conducting an annual risk analysis by implementing a significantly higher assessment frequency. Rather than relying on a static, once-a-year review, the company structurally feeds insights from ongoing supplier meetings and factory audits into a tri-annual evaluation cycle.

"In regular supplier meetings and factory audits within TenneT's qualification system, suppliers are regularly surveyed and checked as to whether the relevant standards are being met."

PRACTICE **P026**

Risk Analysis – Event-Driven

ADOPTION RATE

38.6% (98/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 4**	CSDDD **Art. 8**

DEFINITION

Company conducts additional risk analyses triggered by material changes in circumstances – such as entering new markets, acquiring new suppliers, or responding to geopolitical events that alter supply chain risk profiles.

WHY THIS MATTERS

Supply chains do not wait for the annual calendar – a geopolitical crisis, a new sourcing relationship, or a credible report of violations can shift risk exposure between scheduled reviews. Stronger practice names the trigger categories explicitly rather than relying on a generic commitment to ad-hoc review.

GOOD PRACTICE EXAMPLE

JENOPTIK AG interprets the requirement for event-driven risk analyses proactively by triggering them based on major global geopolitical developments, rather than solely relying on internal business changes or specific grievance reports. In response to international crises, the company systematically reassessed its exposed supply chains to account for new vulnerabilities.

"An event-driven risk analysis was conducted due to the escalation of the Middle East conflict and the Russia embargo. Due to the changed risk situation of suppliers in Israel, existing supply relationships were reviewed and a concrete risk analysis was carried out."

PRACTICE **P027**

Risk Analysis – Own Business Area

ADOPTION RATE

99.2% (252/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 1**	CSDDD **Art. 8**

DEFINITION

Risk analysis covers the company's own business operations – its facilities, workforce, and direct activities – not only its supply chain.

WHY THIS MATTERS

Own-operations coverage is effectively universal – adopted at the same rate as the overall risk analysis obligation. The analytical question is therefore not whether own operations are included, but whether the analysis treats them with the same rigour as supplier tiers: a dedicated assessment of workforce conditions, facilities, and operational practices, rather than a pro forma confirmation that own operations are in scope. Adoption is near-universal at 99.2% (252/254).

GOOD PRACTICE EXAMPLE

Technische Werke Dresden GmbH conducts a granular risk analysis for its own business area by first categorizing all business units' activities into commercial and industrial roles. Based on this categorisation, the Human Rights Officer develops specific risk profiles through structured expert interviews with relevant department heads (e.g., occupational safety, environmental protection, compliance), mapping potential risks based on severity and likelihood while explicitly distinguishing between gross and net risks.

"The respective risk values are divided into gross and net values. The gross values reflect the risks fundamentally present in the relevant activity, and the net values represent the residual risk remaining after taking into account existing controls and measures."

PRACTICE **P028**

Risk Analysis – Direct Suppliers

ADOPTION RATE

99.2% (252/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 1**	CSDDD **Art. 8**

DEFINITION

Risk analysis covers the company's direct (Tier 1) supplier relationships – those with whom the company has a direct contractual relationship. Coverage is typically assessed through supplier self-assessments, audits, or systematic risk screening applied to the full direct supplier base or a risk-stratified subset.

WHY THIS MATTERS

Direct suppliers are the statutory baseline – the tier over which companies have the most direct leverage through contracts, purchasing terms, and audit access. At this tier, coverage is effectively universal – meaning the analytical differentiator is not whether Tier 1 is included, but how coverage is operationalised: how many suppliers, which segments, on what criteria. BAFA guidance has clarified that Tier 1 coverage must be risk-based, not generic – companies are expected to prioritise the suppliers, segments, and product categories where risks are most likely to occur, rather than applying blanket questionnaires across the full supplier base. Having clear risk criteria is therefore analytically crucial. Adoption is near-universal at 99.2% (252/254).

GOOD PRACTICE EXAMPLE

RWE Aktiengesellschaft evaluates its direct suppliers through a highly structured, three-tiered risk analysis and prequalification process. The assessment scales from basic media screenings to extended self-disclosure questionnaires, and finally to an advanced check for suppliers exhibiting elevated risks. As the report outlines:

"The Advanced Check is the responsibility of RWE AG's Human Rights Expert Team. It is a detailed questionnaire that is specifically tailored to the situation and the supplier to be checked, which is designed to identify environmental and human rights risks."

PRACTICE **P029**

Risk Analysis – Indirect Suppliers

ADOPTION RATE

42.9% (109/254)

UNGP **GP 17–18**	LkSG **§9**	CSDDD **Art. 8**

DEFINITION

Risk analysis extends to indirect (Tier 2 and beyond) suppliers – going beyond the statutory minimum to cover deeper tiers of the value chain where some of the most severe human rights risks are concentrated.

WHY THIS MATTERS

The most severe human rights risks – e.g. child labour in raw material extraction, forced labour in agriculture, unsafe processing conditions – are likely to be concentrated in indirect supply chains, not at the direct supplier tier. The 56-point gap between direct and indirect coverage means most companies are systematically absent from the tiers where risk is most acute.

GOOD PRACTICE EXAMPLE

adidas AG proactively extends its risk analysis and due diligence deep into its indirect supply chain, specifically targeting Tier 2 (T2) and Tier 3 (T3) suppliers. To achieve this, the company employs a strict nomination process and transparency requirements that bridge the gap where direct contractual relationships are absent.

"While we do not have a direct contractual relationship with T2 material suppliers, we follow a nomination process whereby our T1 manufacturers source fabrics and materials only from T2 suppliers specifically selected by adidas. These selected textile suppliers are audited annually to ensure full compliance with our workplace standards. Our T2 partners are also required to disclose their sourcing activities and material transactions with T3 suppliers, as well as the origin of materials sourced for yarn production."

PRACTICE **P030**

Risk Analysis – Value Chain Perspective

ADOPTION RATE

46.9% (119/254)

UNGP **GP 17–18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Risk analysis takes an explicit value chain perspective, mapping risks across the full sequence from raw material extraction through production, logistics, and end use – rather than focusing only on immediate supplier relationships.

WHY THIS MATTERS

A supplier-by-supplier approach to risk analysis can miss structural risks that span multiple tiers. A value chain perspective asks where the most severe risks arise across the entire production system – and follows those risks regardless of the contractual tier at which they sit. P030 slightly exceeds indirect supplier coverage because the two practices measure different things: a value chain perspective can be satisfied through commodity-level tracing – mapping cobalt to the refinery, cotton to the gin – without a systematic sub-tier supplier programme.

GOOD PRACTICE EXAMPLE

Knorr-Bremse AG extends its risk analysis across the entire value chain by specifically tracing high-risk raw materials down to the deepest tiers, such as the smelter and refinery level. The company utilizes the Conflict Minerals Reporting Template (CMRT) and the Extended Minerals Reporting Template (EMRT) to gather origin data for minerals such as 3TG, cobalt, and mica from its suppliers.

"In an annual survey, we require information from direct suppliers with 3TG relevance on the origin of the minerals used, by means of the Conflict Minerals Reporting Template (CMRT)."

B. Risk Dimensions – P031–P033

PRACTICE **P031**

Country Risk Considered

ADOPTION RATE

96.5% (245/254)

UNGP **GP 17–18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Risk analysis incorporates country-specific risk data – including governance indicators, rule of law assessments, prevalence of forced and child labour, and human rights conditions – to calibrate risk exposure by geography.

WHY THIS MATTERS

Country context is one of the most predictive dimensions of human rights risk – the same sector activity can carry fundamentally different profiles depending on where it occurs. Country risk assessment directs attention toward the geographies where structural conditions for violations are most concentrated. Adoption is near-universal at 96.5% (245/254).

GOOD PRACTICE EXAMPLE

Heidelberg Materials AG conducts a highly granular assessment of country-specific risks by leveraging a broad and diverse spectrum of internationally recognized indices and government reports. To build a robust profile of the countries in its operations and supply chain, the company aggregates specific thematic data, stating:

"To accurately assess the situation in the countries in which the company operates, country ratings, US State Department country reports on human rights, the Child Labour Index, the Corruption Perceptions Index, and the Global Slavery Index are consulted."

PRACTICE **P032**

Sector Risk Considered

ADOPTION RATE

92.9% (236/254)

UNGP **GP 17–18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Risk analysis incorporates sector-specific risk data – including known patterns of human rights violations associated with particular industries, commodities, and production processes.

WHY THIS MATTERS

Sector membership is a powerful predictor of exposure to specific human rights risks. Stronger practice cross-references sector risk against the company's specific procurement categories rather than applying generic sector classifications – a chemicals company sourcing both solvents and agricultural inputs faces materially different sector risks within the same sector.

GOOD PRACTICE EXAMPLE

Bayer AG systematically evaluates sector-specific vulnerabilities by collaborating with the external expert organization BSR (Business for Social Responsibility) to construct a bespoke sustainability risk framework. This framework explicitly isolates 'category risk' to analyse the specific industry in which a supplier operates, breaking down the assessment into distinct environmental, social, and governance dimensions. As detailed in the report:

"The risk framework focuses on the industry in which the supplier operates – category risk – and on the sustainability risk of the respective country. Both risk factors are based on different risk dimensions such as environmental, e.g. climate and energy, social, e.g. child labour, and governance, e.g. data protection."

PRACTICE **P033**

Product/Service Risk Considered

ADOPTION RATE

68.1% (173/254)

UNGP **GP 17–18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Risk analysis considers risks specific to particular products or services – including the materials, production processes, and commodity chains associated with the company's own product portfolio.

WHY THIS MATTERS

Country and sector analyses establish a structural risk backdrop. Product-level analysis sharpens this by identifying which specific products – and which materials they require – carry elevated risk. Commodity-level analysis by specific material category (cotton, cobalt, palm oil, rubber) is more actionable since it identifies the upstream origin of risk rather than its downstream expression.

GOOD PRACTICE EXAMPLE

adidas AG systematically considers product and material-specific risks by conducting deep-dive analyses into the unique vulnerabilities of the specific raw materials used in its goods, such as cotton, leather, recycled polyester, and natural rubber. The company recognizes that different materials carry distinct risk profiles – such as forced labour in agricultural extraction or deforestation in rubber sourcing – and tailors its supply chain mapping and assessment accordingly. As noted in the report:

"Due to this potential risk of forced and/or child labour linked to the leather industry through the beef and cattle sector, we launched a study on the leather sector in Brazil in 2023 in collaboration with the FLA."

C. Risk Evaluation – P034–P036

PRACTICE **P034**

Severity Assessment

ADOPTION RATE

87.4% (222/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 2**	CSDDD **Art. 8**

DEFINITION

Risk analysis assesses the severity of potential impacts – evaluating how serious a rights violation would be, how many people would be affected, and how reversible the harm would be.

WHY THIS MATTERS

Severity is the primary criterion for risk prioritisation under the UNGPs. Stronger practice anchors severity explicitly to the UNGP scale – scale (how many people affected), scope (how widespread), irremediability – rather than applying a generic impact definition borrowed from financial risk frameworks.

GOOD PRACTICE EXAMPLE

GLOBALFOUNDRIES Management Services Limited Liability Company & Co. KG systematically assesses the severity of potential impacts by explicitly evaluating the three core dimensions of severity: the scale of the violation, the number of people affected, and the irreversibility of the impact. To operationalise this assessment, the company maps these dimensions directly onto the standardized severity categories of the Responsible Business Alliance (RBA) audit framework.

"GF weights and prioritises violations on the basis of the severity of a violation, the number of persons affected, and the irreversibility of the violation. We apply the severity categories used in RBA audits: Priority [...] Major [...] Minor [...]."

PRACTICE **P035**

Likelihood Assessment

ADOPTION RATE

92.9% (236/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 2**	CSDDD **Art. 8**

DEFINITION

Risk analysis assesses the likelihood or probability that identified risks will materialise into actual violations.

WHY THIS MATTERS

Likelihood combined with severity allows the company to distinguish between risks that are severe but remote and risks that are moderate but imminent – a distinction that drives very different prioritisation decisions. Without it, risk analysis produces categories rather than an action sequence.

GOOD PRACTICE EXAMPLE

Nestlé Deutschland AG systematically assesses the likelihood of risks occurring by triangulating abstract risk scores with an evaluation of existing internal processes and concrete historical data from its internal audit programs. Rather than relying on subjective estimates, the company uses this combined operational data to form a robust probability metric. As noted in their report:

"Assessment was carried out using a three-tier score (high, medium, low), a survey of existing regulations, processes and preventive measures, as well as findings from our internal CARE audit programme."

PRACTICE **P036**

Risk Prioritisation

ADOPTION RATE

92.5% (235/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 2**	CSDDD **Art. 9**

DEFINITION

Company explicitly prioritises identified risks – ranking them by severity and likelihood to determine where preventive and remedial resources should be concentrated.

WHY THIS MATTERS

Without explicit prioritisation, every identified risk competes equally for attention – and in practice, the most visible ones win rather than the most severe. Publishing the prioritised risk list – or at minimum the top-tier risks – converts prioritisation from a methodology claim into an auditable output.

GOOD PRACTICE EXAMPLE

Helios Kliniken GmbH structures its risk analysis in distinct phases, explicitly reserving the final evaluation phase for assessing the identified risks based on their impact and probability. To achieve a highly accurate prioritisation, the company breaks down the severity of the impact into three specific dimensions: the scale of the violation, the number of people affected, and its irremediability, which are then weighed against the probability of occurrence.

"This phase looks at the impact on those affected and the likelihood of the risks actually occurring. We then define remedial and preventive measures for prioritized risks."

D. Methodology – P037–P039

PRACTICE **P037**

Risk Analysis Uses External Data

ADOPTION RATE

90.6% (230/254)

UNGP **GP 18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Risk analysis draws on external databases, indices, and intelligence sources – such as country risk ratings, NGO reports, sector-specific risk tools, and commercial due diligence platforms – to supplement internal knowledge.

WHY THIS MATTERS

External data sources provide systematic intelligence that internal processes cannot generate. Companies that rely only on supplier self-reporting or internal knowledge produce a risk picture that reflects what they already know rather than what conditions are.

GOOD PRACTICE EXAMPLE

Uniper SE conducts its abstract supply chain risk analysis by extensively relying on external data, specifically leveraging an external ESG risk platform that systematically evaluates the risk level of every business partner based on massive datasets.

"With expertise in 20 languages and coverage of more than 140,000 public and private companies and 35,000 infrastructure projects, this tool enables comprehensive research into risks."

PRACTICE **P038**

Abstract Risk Analysis

ADOPTION RATE

96.1% (244/254)

UNGP **GP 17–18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Company conducts an abstract (desk-based, top-down) risk analysis – a high-level assessment of sector, country, and product-level risk exposure that serves as an initial filter to identify areas of elevated risk warranting deeper investigation.

WHY THIS MATTERS

The abstract stage is a triage: applied across a large supplier base using publicly available indices, it identifies the relationships worth deeper scrutiny without requiring equal intensity across all of them. Stronger practice documents the indices used, scoring thresholds, and escalation criteria – making the triage transparent rather than implicit. Adoption is near-universal at 96.1% (244/254).

GOOD PRACTICE EXAMPLE

freenet AG conducts its abstract risk analysis by combining objective country and sector-specific parameters to efficiently map general risk exposure across its supplier base. The company acts on this by cross-referencing suppliers located outside of OECD member states with 29 specific high-risk sectors identified in a research report by the Federal Ministry of Labour and Social Affairs (BMAS).

"According to this, an abstract risk was identified if a supplier is not based in an OECD member state and goods were sourced from a risk sector. […] The suppliers associated with an abstract risk were then individually assessed by the responsible procurement department to determine whether they were aware of any specific risks or even violations of protected legal positions."

PRACTICE **P039**

Concrete Risk Analysis

ADOPTION RATE

94.1% (239/254)

UNGP **GP 17–18**	LkSG **§5**	CSDDD **Art. 8**

DEFINITION

Company conducts a concrete (bottom-up, targeted) risk analysis of specific suppliers, products, or relationships identified through abstract analysis as warranting deeper investigation – involving direct engagement, on-site inquiry, or targeted data gathering.

WHY THIS MATTERS

The concrete risk analysis moves from desk-based typology to direct evidence – from structural probability to ground-level fact. Where the abstract analysis asks „where might risks be concentrated?", the concrete analysis asks „what is actually happening in this specific relationship or facility?" The answer requires supplier engagement, site visits, worker interviews, or third-party auditing – a step that almost no company conducting abstract analysis appears to skip.

GOOD PRACTICE EXAMPLE

HOCHTIEF Aktiengesellschaft conducts its concrete risk analysis using a targeted, bottom-up approach to transition from abstract, macro-level data to specific operational realities. To achieve this, the company directly engages relevant internal specialized departments with specific human rights and environmental questionnaires, explicitly evaluating existing preventive measures to calculate precise net risks.

"In a second step, following the abstract risk analysis, a concrete risk analysis was conducted – bottom-up – to identify concrete human rights risks relevant to the Group's business activities."

Deutsche Telekom AG – Risk analysis as an integrated system[2]

Contributed by Deutsche Telekom AG for the UN Global Compact Germany Network domain report series. Company-authored account; not independently coded or verified.

Deutsche Telekom describes its risk analysis not as a standalone compliance exercise, but as the foundation for integrating human rights considerations into decision-making across the organization. Rather than remaining within reports, risk analysis results are systematically fed into internal processes – procurement, M&A, and increasingly sales and customer management– so that relevant risks are considered whenever decisions are made.

To operationalise this, the company combines its regular annual risk analysis with more granular, data-driven monitoring. An external risk-monitoring tool continuously flags incidents linked to suppliers; analysts identify these incidents and provide case-based insights that go beyond abstract country or sector risks. Consolidating such cases over time allows the company to identify recurring risk patterns and to engage directly with suppliers on specific issues. Procurement teams and human rights experts jointly assess and prioritise cases, making risks more tangible and allowing the company to address them earlier rather than reactively.

Ad hoc analyses remain a second key component, primarily triggered through the grievance mechanism. Incoming reports are assessed by a dedicated expert team that evaluates their relevance and arranges appropriate follow-up. Investigations are typically carried out at the level of local business units, while central teams provide guidance and maintain consistency. The combination of routes – regular, continuous, and ad hoc – is designed to uncover risks that may otherwise remain invisible in complex, multi-tier supply chains, and to feed those risks back into the regular analysis and supplier dialogues.

Beyond the supply chain, the company is also extending risk analysis to downstream activities. Human rights considerations are being integrated into customer and product-related assessments – for example, analysing how products might be used and whether certain customer groups could be linked to risks – marking a shift towards a more holistic understanding of human rights risks across the value chain.

The case illustrates a system-level proposition consistent with this report's central finding: the effectiveness of risk analysis lies less in any single procedural element than in the integration between them. Where regular assessment, continuous monitoring, grievance-triggered analysis, and downstream scope are tied together, risk analysis can move from a periodic mapping exercise to a dynamic input into business decisions.

2 The report's quantitative findings chart the field-wide state of risk analysis practices: what is established, what is fragile, and what is absent across the 254 companies in the sample. They do not – and cannot – capture how well individual companies integrate the elements of risk analysis into a functioning system. This section presents the first of two company cases, contributed by the company itself as part of a UN Global Compact Germany Network initiative to feature at least one case study per domain report in this series. The case is a first-person account of the company's approach, not an independent assessment: it has not been coded against the study's 166-item framework and it has not been externally verified. Subsequent domain reports in this series will feature equivalent company-contributed cases in governance, prevention, remediation, and grievance mechanisms. This case study draws on a structured interview with the company conducted by the research team.

E. Accountability – P040

PRACTICE **P040**
Risk Owners Assigned

ADOPTION RATE
83.1% (211/254)

UNGP **GP 17–18**	LkSG **§4 Abs. 3**

DEFINITION

Company assigns specific individuals or roles as owners for identified risks, making named functions responsible for monitoring and managing those risks over time.

WHY THIS MATTERS

Unless a named person or function owns a risk – watching whether it worsens, escalating when it does, confirming that preventive measures were implemented – the risk register is a list with no one responsible for what is on it.

GOOD PRACTICE EXAMPLE

adidas AG operationalises accountability by decentralizing its risk management and formally assigning specific "risk owners" within each relevant business unit. These individuals receive targeted briefings and are tasked with overseeing human rights and environmental due diligence within their specific domains. As noted in their report:

"We took further steps to improve our risk management. These include in particular [...] the selection and appointment of so-called ‚risk owners' in each relevant business function, who are responsible for identifying, assessing and managing negative human rights and environmental risks in their respective areas of operational responsibility."

III. PRACTICE LANDSCAPE: STAKEHOLDER ENGAGEMENT & RIGHTS FOCUS

GP 17 is explicit that identifying human rights impacts requires "meaningful consultation with potentially affected groups and other relevant stakeholders." This section examines the five practices and one grouped indicator that capture how companies integrate stakeholder knowledge into their risk analysis – and which specific rights categories they assess. The two sub-sections are connected: meaningful rights coverage requires knowing which rights are most at risk in a given context, and that knowledge is most reliably generated through engagement with those exposed to those risks. Rights-specific coverage (P047–P053) is therefore both a product of good stakeholder engagement and a measure of analytical depth in its own right. Under the LkSG, §5 requires companies to involve relevant stakeholders in risk analysis; the CSDDD goes further, explicitly requiring meaningful engagement with affected persons and their representatives.

A. Stakeholder Input – P041–P044

PRACTICE **P041**

Stakeholder Consultation in Risk Analysis

ADOPTION RATE

50.4% (128/254)

UNGP **GP 18**	LkSG **§5**	CSDDD **Art. 13**

DEFINITION

Company consults relevant stakeholders – including NGOs, trade unions, civil society organizations, and industry groups – as part of its risk analysis, drawing on external perspectives to improve the quality and completeness of the assessment.

WHY THIS MATTERS

A company doing risk analysis without external input is working from its own knowledge of its own supply chain – which is exactly the knowledge most likely to understate risk. NGOs in sourcing countries, trade unions with access to workers, civil society tracking sector conditions see things that supplier questionnaires and commercial databases miss. GP 17 treats this consultation not as supplementary but as intrinsic to identifying impacts – yet it remains the exception rather than the rule in this sample.

GOOD PRACTICE EXAMPLE

EnBW Energie Baden-Württemberg AG integrates external stakeholders, particularly vulnerable groups and local representatives, directly into its risk analysis and auditing processes. When evaluating supply chain risks, especially in high-risk raw material extraction areas, the company goes beyond speaking merely with the producers to directly engage with local rights-holders. Furthermore, the company initiates targeted multi-stakeholder dialogues on specific salient risks – such as forced labour – to gauge problem awareness and room for action with technical experts and relevant actors.

"During these audits, in addition to discussions with raw material producers, stakeholders such as representatives of trade unions, local communities and local civil society are also interviewed."

PRACTICE **P042**

Worker Representatives Consulted

ADOPTION RATE

45.3% (115/254)

UNGP **GP 18**	LkSG **§5**	CSDDD **Art. 13**

DEFINITION

Worker representatives – including works councils, trade unions, and employee representatives – are consulted as part of the risk analysis, providing direct worker perspective on conditions and risks.

WHY THIS MATTERS

Workers know things that audits miss: the informal pressure not to raise complaints, the violation that occurred last Tuesday, and the safety hazard that management does not notice. Works councils and trade unions have the mandate and access to surface that knowledge – but only if they are asked. The adoption rate falls below even stakeholder consultation – notable given that worker representatives are more directly accessible to most companies than external civil society organizations.

GOOD PRACTICE EXAMPLE

Heidelberg Materials AG integrates the perspectives of worker representatives directly into its core due diligence and risk identification processes. The company employs both quantitative and qualitative data collection methods, explicitly conducting targeted interviews with trade union representatives to map and identify early-stage human rights risks.

"Through interviews with operational and administrative employees, trade union representatives and managers, we can both identify risks at an early stage and detect possible violations."

PRACTICE **P043**

Complaints Considered in Risk Analysis

ADOPTION RATE

70.9% (180/254)

UNGP **GP 17–18**	LkSG **§5/§8**	CSDDD **Art. 8**

DEFINITION

Information from the company's complaint and grievance mechanism is fed back into the risk analysis, using complaint data as a signal about where risks may be materialising or intensifying.

WHY THIS MATTERS

Complaint data is among the most direct evidence of where harm is occurring – not predicted, documented. A pattern of complaints from a particular supplier or region is a real-time signal, not a lagging indicator. The practice sits just below the field-standard threshold: a significant minority of companies run their grievance mechanism and risk analysis as parallel systems that rarely speak to each other.

GOOD PRACTICE EXAMPLE

Arbeiterwohlfahrt Landesverband Saarland e.V. systematically integrates its grievance mechanism into its risk analysis by establishing a clear internal feedback loop. The Human Rights Officer, who oversees the complaints procedure, is responsible for the direct communication of insights gained from grievances to the relevant operational departments.

"The Human Rights Officer manages the complaints procedure, proposes measures to the management to eliminate or reduce risks, monitors their implementation, and reports back on compliance."

PRACTICE **P044**

Affected Persons Input in Risk Analysis

ADOPTION RATE

47.2% (120/254)

UNGP **GP 18**	LkSG **§5**	CSDDD **Art. 13**

DEFINITION

Company obtains direct input from potentially affected persons – including workers, community members, and vulnerable groups – as part of its risk analysis, ensuring those most exposed to risks have a voice in how those risks are assessed. Unlike P041, which covers external stakeholders generally, P044 specifically measures whether potentially affected persons – the rights-holders themselves – have a direct voice in the analysis.

WHY THIS MATTERS

GP 17 is unambiguous: due diligence requires engagement with potentially affected people, not analysis conducted about them at a distance. A worker survey in a sourcing community, a focus group with smallholder farmers, a consultation with a migrant labour NGO – these generate information that no country risk index captures. Fewer companies obtain this input than do not.

GOOD PRACTICE EXAMPLE

Deutsche Post AG systematically integrates the direct input of potentially affected persons into its risk assessment and monitoring processes across both its own operations and its supply chain. Internally, the company utilizes an annual, Group-wide employee opinion survey that empowers all employees to anonymously rate their working conditions, the results of which are used to discuss findings in teams and derive targeted action plans. Externally, the company mandates that the voices of the actual rights-holders are heard during supply chain evaluations, stating:

"In onsite audits, the supplier's workers are also invited and their perspective is considered."

B. Salient Risks – P045

PRACTICE **P045**
Salient Risks Identified

ADOPTION RATE
87.0% (221/254)

UNGP **GP 17–18**	LkSG **§5 Abs. 2**	CSDDD **Art. 8**

DEFINITION

Company explicitly identifies its most salient human rights risks – those representing the greatest severity of potential impact on people – using the UNGP concept of salience as the organising principle for risk prioritisation.

WHY THIS MATTERS

Salience under the UNGPs is a people-centred concept: risks are prioritised by severity of impact on people – scale, scope, irremediability – rather than by financial or reputational exposure to the company. A company prioritising by business materiality may end up focused on different risks, in different locations, affecting different people.

GOOD PRACTICE EXAMPLE

INDUS Holding AG identifies salient human rights risks – specifically those with severe and irreversible consequences, such as child and forced labour – rather than treating them as statistically diluted within its quantitative risk scoring system. The company explicitly overrides standard mathematical averages for these severe impacts to force them to the top of the priority list, stating:

"If such an abstract risk exists for a company under consideration (supplier), that company is classified as correspondingly high-risk, so that it is not excluded by the mathematical calculation."

C. Rights Issues Assessed – P047–P053

PRACTICES **P047–P053**
Rights Issues Assessed

UNGP **GP 17–18**	LkSG **§2**	CSDDD **Art. 8**

DEFINITION

Company explicitly assesses specific categories of human rights and environmental risk – including child labour, forced labour, discrimination, occupational safety and health, fair wages, freedom of association, and environmental risks – as required by the LkSG's enumeration of protected rights under §2.

WHY THIS MATTERS

Named, issue-specific assessments produce a different and more actionable risk picture than generic analysis. The assessment applies across all tiers: own operations, direct suppliers, and – where applicable – indirect suppliers. A company that assesses child labour risk knows where to look; one that assesses „human rights risk" generically does not.

CODE	RIGHTS ISSUE	ADOPTION	N
P047	Child Labour	79.9%	203/254
P048	Forced Labour	81.5%	207/254
P049	Discrimination	90.5%	230/254
P050	OSH (Occupational Safety & Health)	96.1%	244/254
P051	Fair Wages	84.2%	214/254
P052	Freedom of Association	78.7%	200/254
P053	Environmental Risks	90.5%	230/254

Average across seven categories: 85.9%. OSH leads at 96.1%; Freedom of Association lags at 78.7%.

GOOD PRACTICE EXAMPLE

Dürr AG identifies freedom of association risk with geographic specificity – naming the countries and regions where structural conditions make this right most vulnerable, and integrating this assessment into its prioritised risk framework. This approach moves beyond checkbox inclusion of freedom of association to a geographically calibrated assessment of where the risk actually concentrates.

"With a global presence at 142 locations in 32 countries, we see potential risks in the area of disregard for freedom of association and the right to collective bargaining particularly in emerging and developing countries."

IV. §9 SUBSTANTIATED KNOWLEDGE – INDIRECT SUPPLIER TRIGGER

§9 LkSG operates differently from §5. Where §5 defines the baseline scope and cadence of risk analysis, §9 creates a reactive obligation: when a company obtains substantiated knowledge (substantiierte Kenntnis) of a potential violation by an indirect supplier, it must immediately conduct a risk analysis and take appropriate action. P046 captures whether companies have built the procedural readiness to act on that trigger – not whether the trigger has in fact fired.

PRACTICE **P046**

Substantiated Knowledge of Indirect Supplier Violations

ADOPTION RATE

53.1% (135/254)

UNGP **GP 17–18** | LkSG **§9**

DEFINITION

Company has documented procedures for responding to substantiated knowledge – verifiable indications – of human rights or environmental risks or violations involving indirect suppliers. Unlike the §5 practices which define the baseline scope and methodology of risk analysis, this is a reactive obligation whose adequacy is assessed against the quality of the response procedure, not the frequency of its activation.

WHY THIS MATTERS

Most companies document §9 readiness as a general commitment; fewer define what constitutes a verifiable indication or specify the response timeline. The gap between a general statement and an operationalised trigger procedure is the gap between preparedness and compliance.

GOOD PRACTICE EXAMPLE

BASF SE exemplifies a rigorous response to substantiated knowledge of violations by an indirect supplier by conducting immediate, on-site event-driven risk analyses and taking decisive action. Upon becoming aware of severe labour violations at indirect seed farms in Brazil, the company halted work, engaged local authorities, and terminated the relationship with uncooperative partners while implementing strict remedial measures with others.

"After becoming aware of a case of undignified working conditions and underage labour in Uruguaiana/Brazil [...] we proactively approached the responsible authorities and evaluated the events on site in an in-depth risk analysis. The work was stopped immediately and the contract with one of the two farms was terminated as it was not possible to deal with the incidents constructively."

Daimler Truck Holding AG – Approaches to ad-hoc risk analysis[3]

Daimler Truck, one of the world's largest commercial vehicle manufacturers, complements its regular human rights risk analysis with event-driven (ad hoc) assessments triggered by specific risk indications, such as inputs from its grievance mechanism, NGO reports or media coverage. While the regular risk analysis primarily focuses on Tier 1 suppliers, risks at deeper supply chain levels often only become visible through additional information provided by external stakeholders or public sources, resulting in targeted ad hoc analyses and due diligence activities. The transport and logistics sector is used here as an example, given its close link to the company's products and its significance in the regular risk analysis.

Given its large supplier base, Daimler Truck relies on a combination of standardized screening and case-specific ad hoc analyses to identify relevant risks. Upon receipt of a report, the company conducts an ad hoc risk analysis to assess the credibility, scope and potential severity of the issue. This structured preassessment allows Daimler Truck to focus on specific risk situations by identifying the affected business relationships, the potentially impacted rights and rights holders, as well as relevant information already available through existing due diligence processes, such as supplier questionnaires or audit reports. It provides a more differentiated view of the risk exposure and helps determine whether, and to what extent, further measures are required, including direct engagement with the supplier.

Based on this assessment, Daimler Truck typically engages with the relevant Tier 1 supplier, who is also requested to involve any affected subcontractors. Depending on the nature and severity of the issue, the company seeks clarification, requests statements, and works collaboratively with suppliers to develop and implement appropriate measures. Especially in urgent cases, early and direct engagement enables faster clarification and more effective risk mitigation. This case-based and dialogue-driven approach supports remediation, strengthens accountability, and fosters trust along the supply chain.

Importantly, insights gained from individual ad hoc risk analyses are also reviewed in a broader context. A cross-case analysis over time can shed light on recurring patterns and underlying structural factors that may influence risk exposure and are not always fully captured through standard risk assessments alone. In this respect, experience in the transport and logistics sector has highlighted the importance of consistent implementation and enforcement of standards across complex supply chain structures, including subcontracting models.

As such challenges are often systemic in nature and extend beyond the sphere of influence of individual companies, Daimler Truck decided at an early stage to complement its own due diligence efforts with collective approaches. In the area of the transport and logistics sector, the company therefore actively participates in cross-industry initiatives such as the Responsible Trucking Initiative (RTI) of CSR Europe. This initiative brings companies together to promote shared standards and worker-driven monitoring tools (so-called "Spot Checks"), with the aim of collectively improving working conditions for drivers. By pooling experience and aligning efforts, such collaborations help address root causes and support progress at a broader, sectoral level.

Overall, this example illustrates that ad hoc risk analyses are not merely a reactive tool, but an essential complement to regular risk assessments. They enable targeted responses to concrete incidents, support constructive engagement with suppliers, and – crucially – help identify systemic issues that can be addressed more effectively through collective action and shared responsibility.

3 See footnote 2 for the methodological framing.

V. EFFECTIVENESS MEASUREMENT

GP 20 requires companies to track the effectiveness of their human rights due diligence responses. This section assesses four indicators that together capture whether risk analysis findings feed back into management action.

A. Effectiveness Indicators

INDICATOR **E003**

Violation Recurrence Tracked

ADOPTION RATE

10.6% (27/254)

UNGP **GP 20**	LkSG **§10**	CSDDD **Art. 15**

DEFINITION

Company tracks whether violations identified in risk analysis or audits recur after remediation measures have been taken – using recurrence rates as an indicator of whether preventive measures are actually working.

WHY THIS MATTERS

A violation that does not recur after remediation is evidence of an effective response. One that recurs is evidence that the underlying condition was not addressed – only papered over. Without tracking recurrence, a company cannot tell the difference – and the data suggest most cannot: recurrence tracking is among the least-adopted effectiveness indicators in this domain.

GOOD PRACTICE EXAMPLE

HOCHTIEF Aktiengesellschaft systematically tracks the recurrence of violations by embedding past incidents directly into the subsequent year's risk assessment matrix. Whenever a violation occurs, the company conducts a root-cause analysis, implements countermeasures, and then automatically flags that specific issue as a high risk for the following year to monitor if it repeats. As their report states:

"A violation would be classified as a high risk in the following year and checked as to whether the violation recurred or whether the previously taken measures were sufficient to prevent recurrence."

INDICATOR **E005**

Risk Prediction Validated

ADOPTION RATE

28.7% (73/254)

UNGP **GP 20**	LkSG **§10**	CSDDD **Art. 15**

DEFINITION

Company validates whether its risk predictions proved accurate – checking whether the areas identified as high-risk in its analysis actually produced violations or incidents, and using this feedback to improve future assessments.

WHY THIS MATTERS

Risk analysis is a prediction. Validation asks whether predictions proved correct – if areas flagged as high-risk produce no violations while violations emerge in areas flagged as low-risk, the model is pointing in the wrong direction. Few companies have built the feedback loop to find out.

GOOD PRACTICE EXAMPLE

Zalando SE systematically evaluates the outcomes of its grievance mechanism on a quarterly basis to identify trends and patterns regarding human rights and environmental issues. The company then uses this real-world monitoring data to cross-reference and validate its initial risk predictions, checking whether its targeted preventive measures align with the operational areas where proven violations actually originate. As their report states:

"In this way, we identify trends and patterns by means of which we can check whether our preventive measures correspond to the areas from which actual proven violations ultimately originate."

INDICATOR **E016**

Audit Findings Severity Tracked

ADOPTION RATE

10.2% (26/254)

UNGP **GP 20**	LkSG **§10**	CSDDD **Art. 15**

DEFINITION

Company tracks the severity of audit findings over time – monitoring whether the proportion of critical and major findings is increasing, stable, or decreasing as a signal of whether conditions in its supply chain are improving.

WHY THIS MATTERS

A supplier with consistently critical findings across multiple audit cycles is not improving – the audit process is cycling without producing change. Stronger practice compares the severity distribution year-on-year, showing whether Critical and Major findings are declining as a proportion. Across the sample, tracking severity trends over time functions as a differentiator rather than a baseline – rare enough that its presence marks a meaningfully more advanced practice posture.

GOOD PRACTICE EXAMPLE

Evonik Industries AG systematically categorizes and tracks the severity of non-compliance issues identified during supplier audits within the Together for Sustainability (TfS) framework. The company classifies audit deviations into 'Minor', 'Major', and 'Critical' findings, prioritizing remediation and defining strict follow-up timelines based directly on this severity level. As detailed in their report:

"Violations identified during audits are categorised as Minor, Major and Critical Findings. The more serious the deficiency, the sooner it must be remedied: Major and Critical findings must be resolved within a shorter timeframe."

INDICATOR **E020**

Supply Chain Transparency Improved

ADOPTION RATE

34.6% (88/254)

UNGP **GP 20**	LkSG **§10**	CSDDD **Art. 15**

DEFINITION

Company tracks whether its efforts to map and gain visibility of its supply chain are producing measurable improvements in transparency – such as increased traceability of commodities to source, higher rates of supplier disclosure, or deeper mapping of sub-tier suppliers.

WHY THIS MATTERS

Supply chain transparency is both a prerequisite for and an output of effective risk analysis. Increasing the proportion of the supply chain that is visible and traceable directly increases the capacity to identify risks – though improved traceability is a measure of analytical capacity, not of actual conditions.

GOOD PRACTICE EXAMPLE

Evonik Industries AG systematically tracks and improves the transparency of its supply chain by quantifying the exact traceability levels of critical raw materials, such as palm oil and its derivatives. The company monitors the origin of these materials across multiple tiers of its indirect supply chain, tracking progress down to the specific extraction and processing sites. As their report details:

"Furthermore, in 2023, 97% of palm-based derivatives were traceable at mill level and 69% at plantation level. Evonik publishes corresponding mill lists."

B. Correlates of Risk Prediction Validation

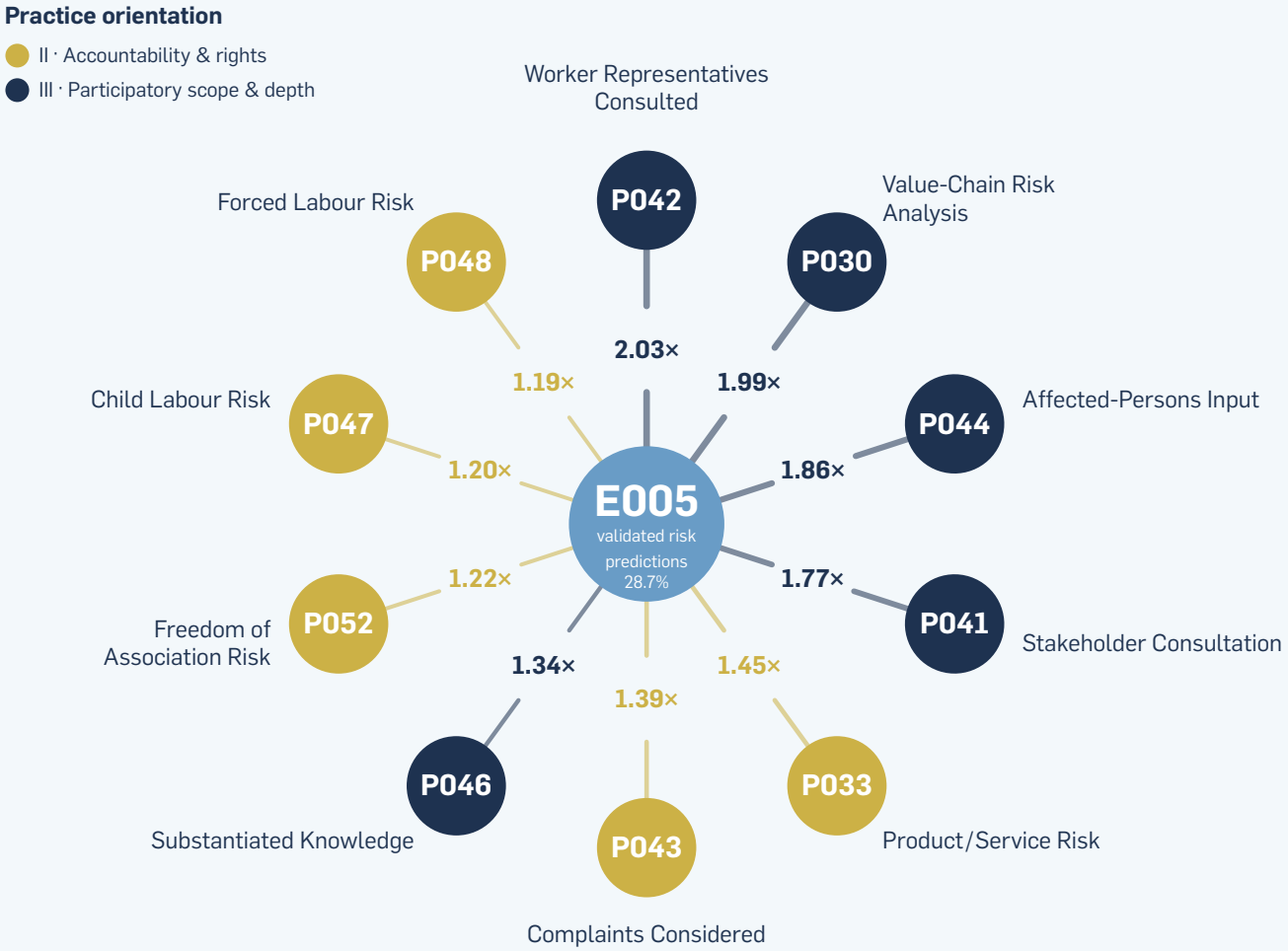
Of the 254 companies, 73 (28.7%) **validate their risk predictions:** they check whether the areas their analysis flagged as high-risk went on to produce the violations it had anticipated (E005). Comparing the practices these validators have adopted against the rest of the sample shows what sets them apart.

The difference is not in the methodology. The **practices that separate the validators are participatory and accountability ones,** not the analytical core. Companies that consult worker representatives (P042) validate at 58.3%, against just 4.3% among those that do not — more than double the sample's 28.7% base rate. Value-chain risk analysis (P030) shows much the same gap (57.1% against 3.7%), with affected-persons input (P044, 53.3%) and stakeholder consultation (P041, 50.8%) close behind. Product- and service-level risk (P033), complaints integration (P043), and §9 substantiated-knowledge procedures (P046) round out the list.

All ten of the strongest predictors come from Orientation III (participatory scope) or Orientation II (accountability and rights); none comes from the methodological core (Figure 2). The pattern is structural rather than coincidental: the core methodology practices are close to universal — 94% adoption on average — so they cannot separate one company from the next. What separates them instead are the practices the field has adopted least, the ones that bring workers, affected persons, and the wider value chain into the assessment. **A company that hears from the people closest to a risk is the one in a position to find out whether it reads that risk correctly.**

FIGURE 2: Risk analysis practices associated with validated risk predictions (E005)

Hub: E005 (Risk Predictions Validated), evidenced by 28.7% of the sample. Spokes: the ten risk analysis practices most strongly associated with measured uptake, sized by lift — the uptake rate among adopters divided by the 28.7% population base. Node colour denotes practice orientation. Source: LkSG disclosure analysis, normalized firm-level matrix, n = 254 companies.



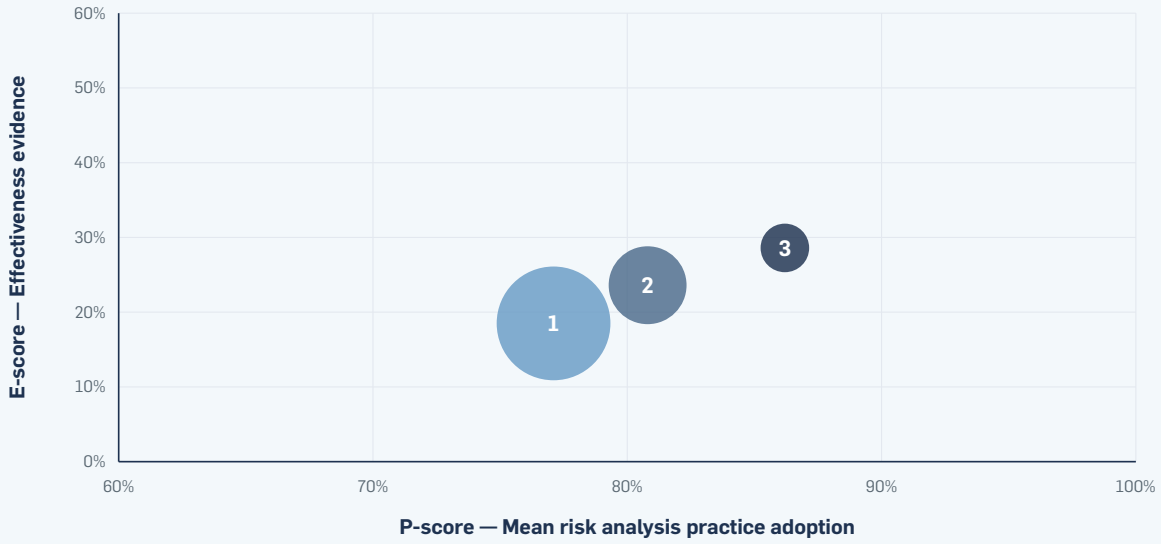
VI. SECTOR & SIZE PERFORMANCE

Figure 1 (above) shows sector-level risk analysis performance, Figure 3 (below) breaks the same P-score and E-score metrics down by employee-count band, isolating the size effect on risk analysis maturity.

FIGURE 3: Size-Band Performance – Risk Analysis P-score vs E-score

P-score (P024–P053, x-axis) vs. E-score (E003, E005, E016, E020, y-axis) by employee size band. Bubble size proportional to n companies. Source: LkSG disclosure analysis, n=254 companies.
Company size correlates with P-score across three size bands, consistent with the expectation that larger companies have greater resources for dedicated risk analysis functions; the three-band design does not support finer-grained inference.

#	Size band (employees)	n	P-score	E-score
1	3,000–10,000	154	77.1%	18.5%
2	10,000–50,000	72	80.8%	23.6%
3	>50,000	28	86.2%	28.6%



VII. CONCLUSIONS

This section synthesises the empirical findings, sets out what substantive risk analysis requires, situates the gaps against the forthcoming CSDDD, and translates them into implications for affected rights-holders.

A. Requirements of Substantive Risk Analysis

The four capabilities described below – accountability, scope, methodology, and stakeholder input – are visible across the practice-level distribution shown in Figure 4.

Across the risk analysis domain, the sample averages a P-score of 79.1% and an E-score of 21.0% – a 58-point gap that is consistent across sectors and size bands. Four capabilities distinguish companies with substantive risk analysis from those with formal compliance – and all four are already documented in this sample, not projected from theory.

Accountability structures that convert analysis into governance. Named risk owners (P040: 83.1%), formal §9 response procedures (P046: 53.1%), documented feedback loops between complaint data and risk registers (P043: 70.9%): these are what convert a risk analysis from a reporting artefact into something managed.

Scope that follows the risk, not the contract. Companies that proactively cover indirect suppliers (42.9%), build a value chain perspective (46.9%), and document §9 response procedures (53.1%) have made a deliberate decision: scope is defined by where risks concentrate, not by where contractual relationships end – a choice the majority of the sample has not yet made. Anticipated CSDDD requirements will extend this expectation, making a risk-based approach to indirect supplier coverage a regulatory standard rather than a leading practice.

Methodology that is structured, transparent, and external-data-grounded. The two-stage methodology – abstract triage (96.1%) followed by targeted concrete investigation (94.1%) – allocates scrutiny proportionately. What differentiates the upper end is not the methodology itself, but the data behind it: commodity-level indices, external platforms, NGO field reporting, a documented sourcing trail. The lower end produces a risk picture that reflects what the company already knows – strong on indexed data, thin on human intelligence.

Stakeholder input as a structural requirement, not an optional step. The clearest differentiator in this domain is whether external stakeholders actually had a voice in the assessment. Stakeholder consultation (50.4%), worker representative input (45.3%), and affected persons engagement (47.2%) remain minority practices – yet GP 17 is explicit that this consultation is not a supplementary activity.

The chart below summarises adoption rates for all 30 risk analysis practices and the four effectiveness indicators covered in this report, grouped by domain. Three patterns – differentiation within the P-series between broadly adopted and minority practices, the asymmetry between P- and E-series adoption, and the concentration of under-adopted practices in scope and participation – organise the analysis that follows.

B. Risk Analysis Orientations: Methodology, Accountability, and Participatory Scope

The 30 practices in this domain can be grouped into three orientations that reflect progressively deeper investment in risk analysis quality. The adoption gradient across orientations maps directly onto the report's central finding: methodology is established; participatory scope and external grounding are not. Figure 5 plots the three orientations on a single adoption axis.

FIGURE 4: Practice & Indicator Adoption at a Glance

Bars show adoption rates (%) for all coded practices and effectiveness indicators. Source: LkSG disclosure analysis, n=254 companies.

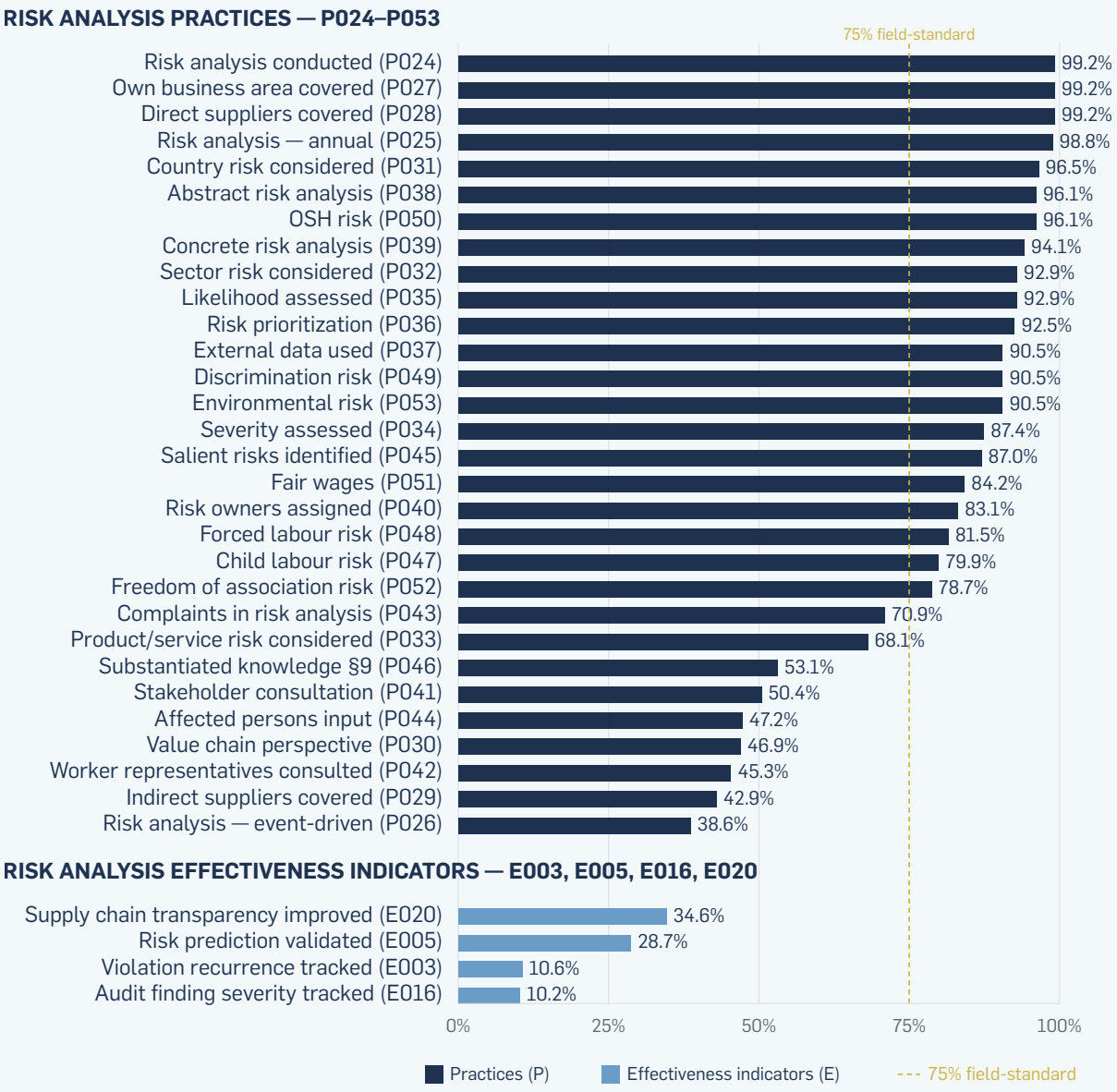
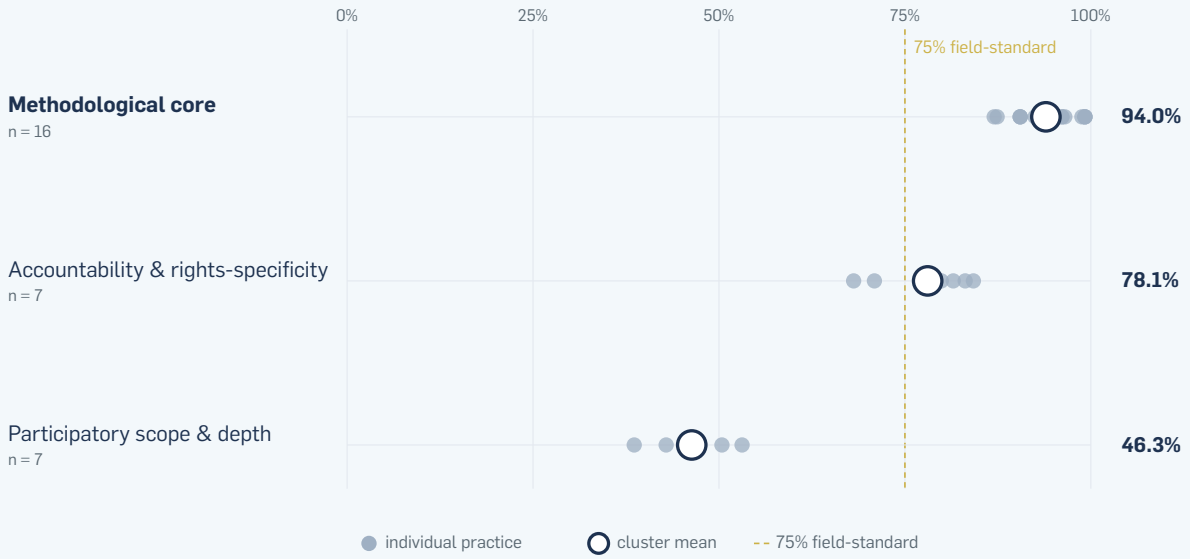


FIGURE 5: Risk Analysis Orientations – Mean Adoption by Cluster



Large dot = cluster mean. Small dots = individual practice adoption rates. Dashed line = 75% field-standard threshold. Source: LkSG disclosure analysis, n=254.
***Orientation I – Methodological core** (16 practices, mean 94.0%): Coverage of own operations and direct suppliers, annual and event-driven cadence, abstract and concrete methodology, evaluation framework (severity, likelihood, prioritisation), external data sourcing, and rights-category identification. Broadly established – these practices constitute the analytical infra-structure of risk analysis across the sample.*
***Orientation II – Accountability and rights-specificity** (7 practices, mean 78.1%): Risk ownership, complaints integration, product and service risk, and issue-specific rights category assessment (fair wages, forced labour, child labour, freedom of association). Above the 75% threshold on average, but several individual practices sit just above it – a fragile field standard.*
***Orientation III – Participatory scope and depth** (7 practices, mean 46.3%): Indirect supplier coverage, value chain perspective, event-driven triggers, stakeholder consultation, worker representatives, affected persons engagement, and §9 substantiated knowledge procedures. Every practice in this cluster sits below the 75% field-standard threshold. This is the dimension on which the CSDDD most directly raises the bar beyond the LkSG baseline.*

C. Implications for Rights-Holders

The companies examined here have broadly and quickly put the basic structure of risk analysis in place. The harder threshold – analysis with enough scope and self-correction to actually identify and track the conditions it means to improve – has not yet been universally reached.

D. CSDDD Outlook

On the procedural core of risk analysis – methodology, severity and likelihood assessment, risk ownership, annual cadence – **companies in this sample are well-positioned for the CSDDD.** Where the CSDDD will require a material departure from current LkSG practice is in three areas that are also this domain's critical gaps.

1. **Scope:** the CSDDD's risk-based approach treats indirect supplier coverage as a function of where risks are severe, not where contractual relationships end. Fewer than half the companies in the sample currently extend systematic analysis beyond direct suppliers.
2. **Stakeholder engagement:** the CSDDD requires meaningful engagement with affected persons as an intrinsic element of the risk analysis – not a supplementary step. Stakeholder consultation (50.4%), worker representative input (45.3%), and affected persons engagement (47.2%) remain minority practices in this sample.
3. **Effectiveness:** the CSDDD places monitoring and evaluation of due diligence adequacy at the centre of compliance. The four effectiveness indicators in this domain – violation recurrence tracking, audit finding severity trends, risk prediction validation, and supply chain traceability – average 21.0% adoption. This is the dimension on which the gap between current LkSG practice and forthcoming CSDDD requirements is widest.

APPENDIX 1: METHODS REFERENCE

SAMPLE COMPOSITION

- **N = 254 companies** drawn from LkSG disclosure registry (all companies ≥3,000 employees, Phase 1 LkSG threshold)
- **16 sectors** (sector classifications sourced from Moody's Orbis and cross-referenced against company self-disclosures)
- **Size distribution:** 3,000–10,000 employees (n=154), 10K–50K (n=72), 50K+ (n=28)
- **Data collection:** June–July 2025 (report identification and coding); analysis period January–March 2026

CODING APPROACH

- Binary presence/absence coding for all 141 practices (P001–P141) and 25 effectiveness indicators (E001–E025)
- Double-coded for Database 2 (typology database); single-coded for Database 1 (LkSG implementation analysis)
- LLM-assisted extraction with human review; latent content analysis applied to maturity scoring
- The LkSG §10 disclosure itself is the GP 21 compliance act; it is not coded as a separate practice

MATURITY TYPOLOGY

Companies are classified into four maturity tiers based on P-score (proportion of all 141 P-series practices disclosed) and E-score (proportion of all 25 E-series indicators disclosed). Thresholds (70%/40%) determined empirically; see the full Methods paper for sensitivity analysis.

LIMITATIONS

- **Disclosure ≠ Implementation:** Presence in disclosures does not establish operational reality
- **Non-response bias:** Early filers over-represent high-risk sectors and larger companies with more mature HREDD systems
- **Binary coding:** Scores reflect disclosure breadth, not implementation depth or quality
- **E-series framing:** E-series indicators measure whether companies have adopted practices to track effectiveness – not whether due diligence structures are actually effective

E-SCORE CONSTRUCTION

The domain E-score reported in this document averages four of the 25 E-series indicators in the full HREDD framework: E003 (violation recurrence tracked), E005 (risk prediction validated), E016 (audit findings severity tracked), and E020 (supply chain transparency improved). These four were selected for substantive relevance to §5 risk analysis: each one measures whether the company has a feedback mechanism testing some aspect of the analysis itself – whether predicted risks materialise, whether recurrence is monitored, whether audit findings inform severity updates, and whether supply chain visibility improves over time. The four-indicator domain E-score (21.0%) is therefore a domain-weighted summary, not a representative average of all E-series indicators (whose sample mean is 30.7% across all 25 items). The higher all-series mean is driven by E021, E022, and E025 – compliance and reporting indicators at 96.5%, 68.1%, and 63.4% respectively – whose near-universal adoption reflects procedural disclosure rather than substantive feedback on the analysis. The 58-point P/E gap reported in this document uses the four-indicator domain E-score; computed against all 25 E-series indicators, the gap narrows to approximately 48 points. The direction and magnitude of the asymmetry are preserved under both constructions.

75% THRESHOLD

The 75% "field-standard threshold" used to identify critical gaps in this domain is a study-specific benchmark chosen as the adoption level at which a practice can be reasonably described as dominant across the sample, approximately one standard deviation below the mean P-series adoption rate in this domain (79.1%). Sensitivity: the five scope-and-participation practices flagged as critical gaps (P029 42.9%, P030 46.9%, P041 50.4%, P042 45.3%, P044 47.2%) remain below threshold at alternative cutoffs of 70% and 80%. Two additional practices (P033 68.1%, P043 70.9%) enter or exit the gap set depending on threshold choice; the substantive findings in this report are robust to these boundary cases.

SAMPLE REPRESENTATIVENESS

The sample of 254 companies is drawn from the LkSG disclosure registry and represents the set of Phase 1 filers (≥3,000 employees) whose 2023 or 2024 disclosures were available for coding at the time of data collection (June–July 2025). Phase 1 covers approximately 900 companies in scope in year one per BAFA reporting, and the sample therefore represents a non-random subset of that population. Early filers tend to over-represent high-risk sectors and larger companies with more mature HREDD systems; the sample is accordingly biased toward the upper end of the field on both practice adoption and effectiveness tracking. Findings should be read as a characterisation of *filed disclosure practice among German Phase 1 LkSG filers*, not as a population-level estimate of HREDD practice in German companies more broadly.

PRACTICE INDEPENDENCE

Several risk analysis practices in the coding framework are structurally dependent rather than empirically independent, because they derive from different facets of the same question in the LkSG disclosure template. Three practices – P024 (risk analysis conducted), P027 (own business area covered), and P028 (direct suppliers covered) – are perfectly collinear in the sample: 253 companies are coded 1 on all three, 1 company is coded 0 on all three, and no company is coded differently across the three (phi = 1.00 for every pairwise comparison). These three practices reflect one disclosure act with three facets; readers should not interpret the "30 risk analysis practices" figure as 30 statistically independent measurements.

Indirect supplier coverage (P029) is hierarchically nested under direct supplier coverage (P028): of the 253 companies covering direct suppliers, 109 also cover indirect suppliers; no company covers indirect without also covering direct. The gap between direct and indirect coverage (99.2% vs 42.9%) therefore captures a decision – whether to extend an existing analysis to the indirect tier – rather than an independent scope variable.

SECTOR ATTRIBUTION

Every company in the sample is assigned to one of 25 granular industry categories and one of three employee size bands (3,000–10,000; 10,000–50,000; >50,000). The granular categories are aggregated to the 16 sectors shown in Figures 1 and 3 using a fixed rule applied consistently across all five domain reports in this series. Six industrial categories – Aerospace & Defense, Electronic & Electrical Equipment, Industrial Engineering, Industrial Support Services, Industrial Transportation, and Industrial Metals & Mining – aggregate to "Industrial Goods"; Chemicals and Pharmaceuticals & Biotechnology aggregate to "Chemicals & Pharma"; Software & Computer Services and Technology Hardware & Equipment aggregate to "Technology"; and Diversified, Research & Education, and Social Services aggregate to "Other Services". Each remaining category maps to a single report sector, several under a shortened label: Food & Beverages to "Food Producers", Gas, Water & Multiutilities to "Utilities", Medical equipment & services / Health care providers to "Health Care", Construction & Materials to "Construction", Real Estate Investment & Services to "Real Estate", and Telecommunications equipment & service providers to "Telecommunications". Automobiles & Parts, Financial Services, Media, Personal Goods, Retailers, and Travel & Leisure retain their labels.

APPENDIX 2: ACRONYMS

3TG	Tin, Tantalum, Tungsten, Gold (conflict minerals)
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle (Federal Office for Economic Affairs and Export Control)
BSR	Business for Social Responsibility
CMRT	Conflict Minerals Reporting Template
CSDDD	Corporate Sustainability Due Diligence Directive (EU)
E-score	Effectiveness score – proportion of 25 E-series effectiveness indicators disclosed by a company
EMAS	Eco-Management and Audit Scheme (EU)
ESG	Environmental, Social and Governance
GP	Guiding Principle (UN Guiding Principles on Business and Human Rights)
HREDD	Human Rights and Environmental Due Diligence
LkSG	Lieferkettensorgfaltspflichtengesetz – German Supply Chain Due Diligence Act (2023)
OECD	Organisation for Economic Co-operation and Development
OSH	Occupational Safety and Health
P-score	Practice score – proportion of 141 P-series practice codes disclosed by a company
RBA	Responsible Business Alliance
Sedex	Supplier Ethical Data Exchange
SMETA	Sedex Members Ethical Trade Audit
UN	United Nations
UNGP/UNGPs	UN Guiding Principles on Business and Human Rights (Ruggie Framework, 2011)

IMPRINT

The UN Global Compact and UN Global Compact Network Germany
The United Nations Global Compact is the world's largest initiative for sustainable and responsible corporate governance. Based on ten universal principles and the 17 Sustainable Development Goals (SDGs), it pursues the vision of an inclusive and sustainable global economy for the benefit of all people. More than 24,500 companies and organizations have already joined the UN Global Compact country networks and contribute to this global vision. The UN Global Compact Network Germany is one of about 65 UN Global Compact country networks and among the largest of them. It currently has more than 1,200 participants — approximately 1,150 companies, ranging from DAX-listed corporations to mid-sized and small enterprises (SMEs), as well as 60 representatives from civil society, academia, and politics.

Aiming to initiate change processes within companies and support the strategic mainstreaming of sustainability, the UN GCD focuses on the topics of human rights and labour standards, environment and climate, and anti-corruption.

Global Compact
Network Germany

HREDD Study Series

DOMAIN REPORTS
- Domain Report 1 — Governance
- Domain Report 2 — Risk Analysis *(this report)*
- Domain Report 3 — Prevention
- Domain Report 4 — Remediation
- Domain Report 5 — Grievance Mechanism

METHODS
- HREDD Performance in Germany — Research Design and Methods

SYNTHESIS
- HREDD Performance in Germany — Cross-Domain Synthesis

Published by
UN Global Compact Netzwerk Deutschland e. V.
Globalcompact.de | LinkedIn

AUTHORED BY
Chris N. Bayer, PhD
Natsuda Uppapong, MSc

Project Managers
Helene Bendig | UN Global Compact Netzwerk Deutschland e. V.
Sarah Hechler | UN Global Compact Netzwerk Deutschland e. V.

Editing
Heather McCrae

Graphic Design and typesetting
ANDREA KRÜGER Design & Kommunikation

June 2026