WHITEPAPER

The German Supply Chain Act: Building your data-driven approach to risk analysis

SAI360
RISK FROM EVERY ANGLE

Contents

SAI360
RISK FROM EVERY ANGLE

Introduction

As of January 1, 2024, the German Supply Chain Act (Lieferkettensorgfaltspflichtengesetz or LkSG) mandates that companies in Germany with over 1,000 employees comply with obligations aimed at ensuring responsible supply chain management. This reflects a scope expansion in line with the Act's phased implementation, which initially applied to firms with over 3,000 employees (01 Jan 2023). According to the Federal Office for Economic Affairs and Export Control (BAFA), the rules now impact roughly 5,200 firms, compared to ~1,300 in 2023.

The LkSG applies to a broad range of entities, including those with their registered office, principal place of business, or administrative headquarters within Germany. Importantly, this threshold is designed to be robust against attempts at circumvention through corporate restructuring or the relocation of employees abroad. Consequently, all business forms, such as limited companies, stock corporations, partnerships, foundations, and associations, fall within the Act's purview.

By the time their respective deadlines hit, firms were expected to have assigned responsibility for monitoring risk management and have functional complaints mechanisms in place. From then on, BAFA expects a timely implementation of the remaining due diligence obligations.[1]

1 https://www.bafa.de/SharedDocs/Downloads/DE/Lieferketten/lksg_ausweitung_anwendungsbereich.html?nn=1468680

What have we learned from a year of implementation for bigger firms?

BAFA audited 486 companies in 2023, with the majority of the controls covering companies from the following sectors: automotive, chemical, pharmaceuticals, mechanical engineering, energy, furniture, textile as well as food and beverage industries.

In line with the phased expectations mentioned above, BAFA focused their efforts on the establishment of risk management responsibility and complaints procedures. The authority seemed encouraged by progress to date, publishing a press release at the end of 2023 highlighting their reflections one year on from the law coming into effect.[2]

Overall, most companies have determined the internal risk management responsibility and thus laid the foundations for further due diligence obligations. In addition, most checked firms have a relatively strong complaints procedure up and running. With that said, BAFA noted a need for improvement with regard to accessibility, visibility and the involvement of potentially affected persons in the design of the complaint procedure.

The outlook for 2024 and beyond

This year, companies in Germany with over 1,000 employees will face the same scrutiny as their larger counterparts, with BAFA assessing their risk management delegation and complaints mechanisms.

For those firms with over 3,000 employees, BAFA has stated that risk analysis procedures will be the primary focus of their audits. By extension, the licensing authority recognizes the foundational role that risk analysis plays in building a robust third party due diligence program.

With all of this in mind, this report will first revisit the broad obligations under LkSG at a high-level before diving into the detail related to the risk analysis expectations set forth in the regulations and additional guidance published since the rules were finalized.

The due diligence obligations under LkSG

It's all about controls...

The duty of care expectations set forth in the Act demonstrates a pragmatic approach to rulesetting. LkSG does not require firms to guarantee that their supply chains are free from human rights violations or adverse environmental impacts. Instead, they need to demonstrate adequate implementation of policies, processes and internal controls to meet the due diligence obligations detailed in Sections 4-10. In principle, therefore, companies cannot be prosecuted if – from an ex-ante perspective – an appropriate and effective measure ultimately fails to have its practical effect.

1 https://www.bafa.de/SharedDocs/Pressemitteilungen/DE/Lieferketten/2023_21_1_jahr_lksg_-_bafa_zieht_positive_bilanz.html#:~:text=Januar%202023%20müssen%20Unternehmen%20mit,Unternehmen%2C%20ohne%20sie%20zu%20überfordern.

LkSG due diligence obligations: Sections 4-10

- **Establishing a risk management system (section 4 (1)):**
  Companies must set up a comprehensive risk management system to identify, assess, and address human rights and environmental risks. This system must be integrated into all relevant business processes and should be regularly reviewed and updated to ensure its effectiveness.

- **Designating a responsible person or persons within the enterprise (section 4 (3)):**
  A designated person or team must be appointed to oversee the implementation of due diligence obligations. This role involves ensuring compliance, coordinating risk management activities, and reporting to senior management.

- **Performing regular risk analyses (section 5):**
  Regular risk analyses must be conducted to identify potential human rights and environmental risks in the supply chain. These analyses should be systematic and consider all levels of the supply chain, including indirect suppliers.

- **Issuing a policy statement (section 6 (2)):**
  Companies are required to publish a policy statement outlining their commitment to human rights and environmental standards. This statement should detail the measures the company will take to fulfill its due diligence obligations.

- **Laying down preventive measures in its own area of business (section 6 (1) and (3)) and vis-à-vis direct suppliers (section 6 (4)):**
  Preventive measures should be implemented within the company's operations and with direct suppliers to mitigate identified risks. This includes training, contract clauses, and support programs to enhance supplier compliance with human rights and environmental standards.

- **Taking remedial action (section 7 (1) to (3)):**
  When violations are identified, companies must take immediate and appropriate remedial actions. These actions should aim to cease the violations and mitigate any adverse impacts. Companies should also develop a plan to prevent recurrence.

- **Establishing a complaints procedure (section 8):**
  An accessible and effective complaints mechanism must be established to allow individuals to report human rights and environmental violations. This mechanism should ensure confidentiality and provide a clear process for addressing complaints.

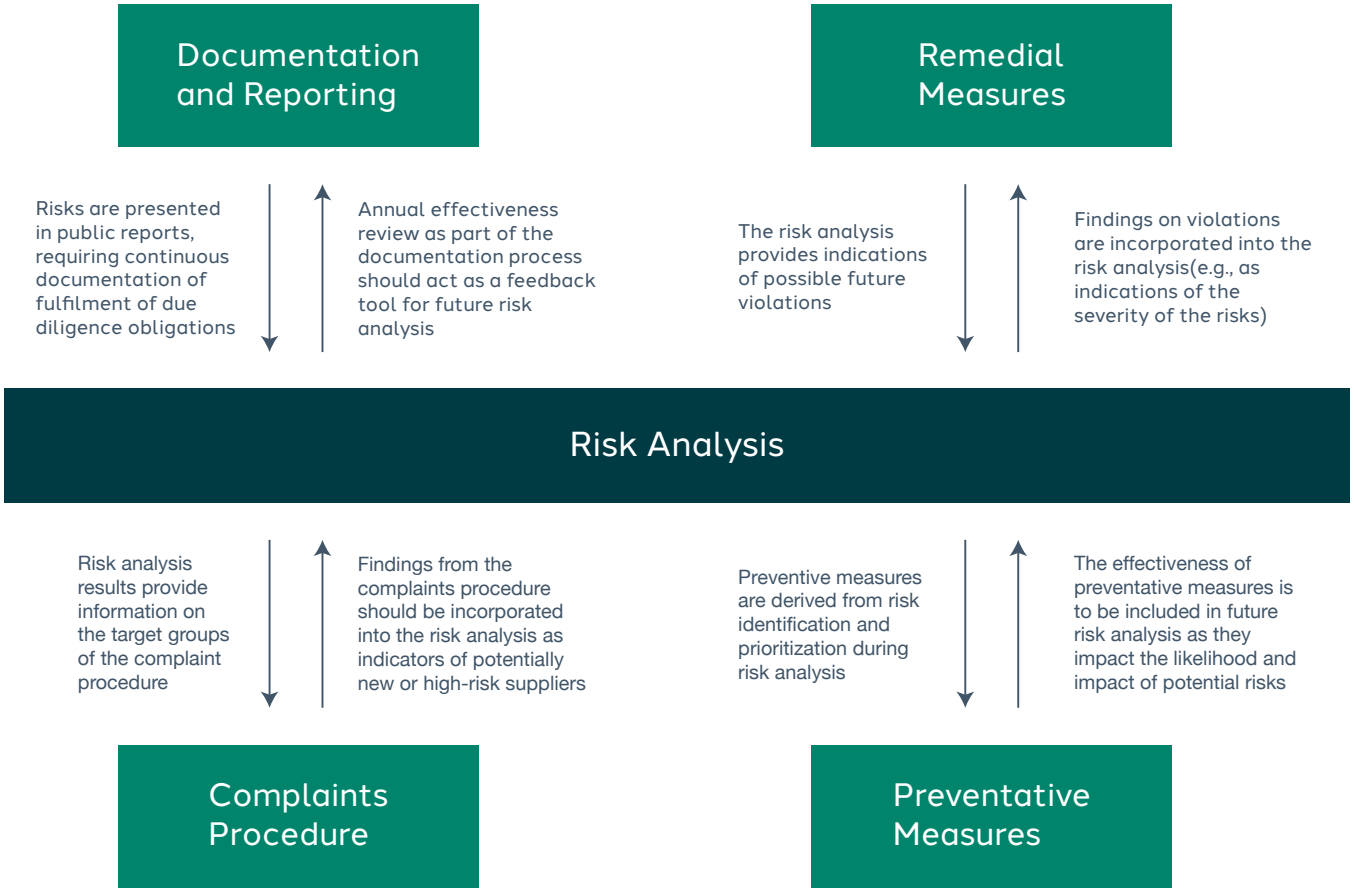
- **Implementing due diligence obligations with regard to risks at indirect suppliers (section 9):**
  Companies must extend their due diligence efforts to include indirect suppliers, particularly when significant risks are identified. This involves conducting risk analyses and implementing preventive and remedial measures as necessary.

- **Documenting (section 10 (1)) and reporting (section 10 (2)):**
  Companies are required to maintain detailed documentation of their due diligence activities and report annually on their compliance. This report should include information on risk management, preventive measures, and remedial actions taken.

Risk analysis deep dive

The relationship between risk analysis and other due diligence elements is dynamic and cyclical. Findings from one process inform the others, creating a feedback loop that enhances the overall effectiveness of the due diligence system. For example, preventive measures derived from risk analysis can lead to fewer violations, reducing the need for remedial actions. Similarly, insights from the complaints procedure can highlight previously unidentified risks, refining future risk analyses and preventive strategies. Such relationships are illustrated in the image below:

Figure 1: Adaptation of "Correlation between risk analysis and other elements of the due diligence process" diagram provided by BAFA

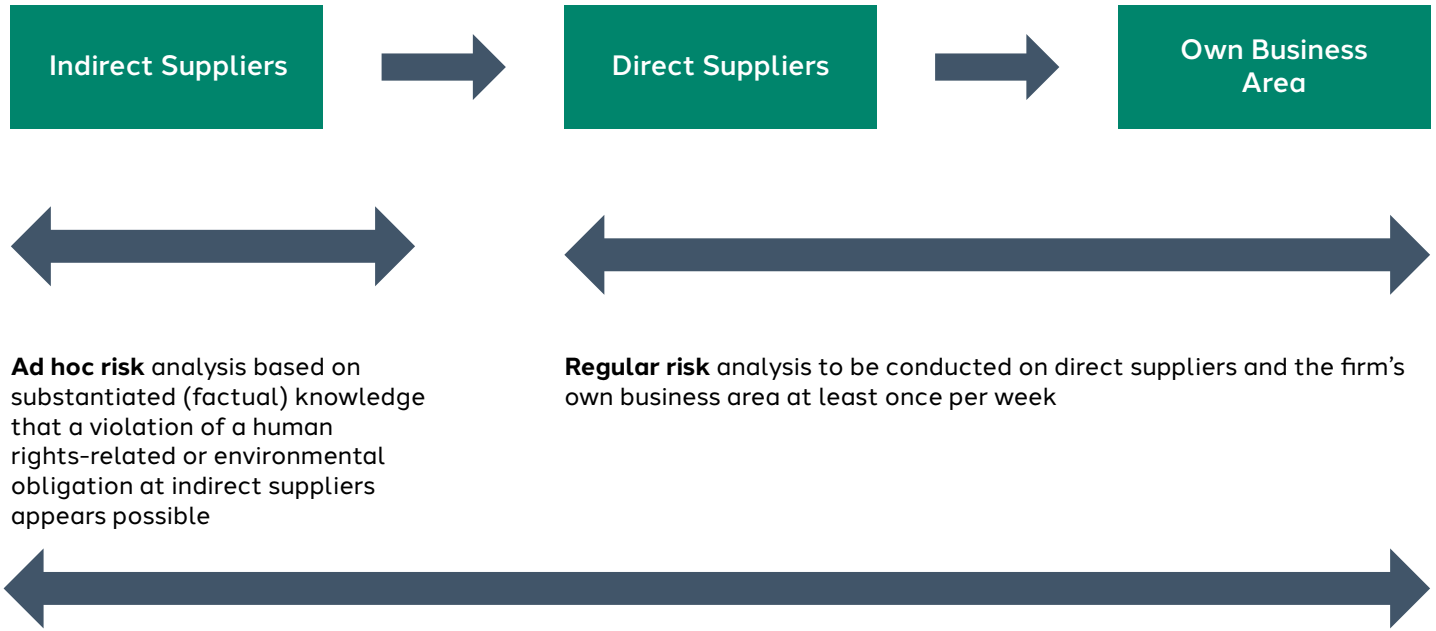


Risk analysis types

LkSG distinguishes between two types of risk analysis which differ both in their occasion and in the areas of the supply chain they have to cover:

- **Regular** (once per year): taking into account all risks in its own business area and at all direct suppliers
- **Ad hoc risk analysis:** triggered by substantiated knowledge of a possible violation of a human rights or environmental obligation at one or more indirect suppliers. Or, when a company expects a significant change in risks or the emergence of new risks along the entire supply chain due to a change in business activity.

Figure 2: Risk analysis frequency for different parts of the value chain



Risk analysis procedures

Companies have a degree of discretion in the way they design and select risk analysis methods. However, they are subject to the condition of "appropriateness". A three-stage template for conducting risk analyses is provided below, derived from the guidance published by BAFA to support firms in this regard.[3]

Appropriateness

Businesses are required to exercise due diligence in their supply chains in a manner that is appropriate (for them). According to Section 3 (2) of LkSG, the appropriate manner of acting in accordance with the due diligence obligations is determined according to:

- The nature and extent of the firm's business activities
- The ability of the enterprise to influence the party directly responsible for the risk or violation of human rights-related or environment-related obligation
- The severity of the violation that can be expected, the reversibility of the violation, and the probability of the occurrence
- The nature of the causal contribution of the enterprise to the risk or violation

1. Conduct an abstract risk assessment

Cross-check information and sources on human rights and environment-related risks with data on the company's own sector, its direct suppliers, one or more indirect suppliers and additional sectors and countries of operation. This forms the initial abstract assessment of risks.

Identify relevant information

- **Human rights risks:** Look for information on labor practices, discrimination, worker safety, community impacts, etc., related to your industry.
- **Environmental risks:** Seek data on pollution, resource usage, biodiversity impact, and climate change associated with your industry.

Gather sources

- **Internal data:** Use company records, reports, and audits that highlight existing risks and compliance issues within your operations, or those of your third parties.
- **Vendor assessments:** During the onboarding process, gather comprehensive data directly from vendors to assess their potential impacts on society and the environment. This may include detailed questionnaires, self-assessment forms, and compliance certificates covering key areas such as labor practices, environmental management systems, human rights policies, and previous incidents related to these domains.
- **External sources:** Collect information from industry reports, academic research, NGO reports, news articles, government databases, and global indices (e.g., Human Rights Watch, Environmental Protection Agency reports).

Cross-check information

- **Sector comparison:** Compare your data with risks identified in similar sectors.
- **Broader context:** Consider data from different sectors that might have overlapping or analogous risks. This helps identify potential blind spots. For example, if your company is in food production, you might look at risks in agriculture and packaging sectors as well.
- **Geographical scope:** Look at risks specific to the countries where you operate.

Form an abstract assessment

- **Synthesize data:** Combine and summarize the gathered information to form a broad overview of potential risks. This initial assessment is "abstract" because it's a high-level view based on available data.
- **Identify patterns:** Look for common risk factors or trends that emerge across your sector and other sectors.
- **Highlight gaps:** Note where data might be lacking or where further detailed analysis is needed.

3 https://www.bafa.de/EN/Supply_Chain_Act/Risk_Analysis/risk_analysis_node.html

2. Concrete risk assessment

Review the risks identified in your abstract assessment and verify their plausibility. Each risk must then be prioritized in a transparent and traceable way using a systematic and consistent approach. BAFA stresses the importance of assessing the likelihood and severity of each violation separately.

Systematically document the risks identified by means of the concrete risk assessment, e.g., in a risk inventory, which typically includes at least the following information:

- **Description of the risk:** What is the risk and how does it manifest?
- **Person(s) responsible:** Who is accountable for monitoring or managing this risk?
- **Weighting:** The importance or priority level of the risk, derived from the likelihood and severity assessment.
- **Preventative measures:** Steps to reduce the likelihood of the risk occurring.
- **Remedial measures:** Actions to take if the risk does materialize to mitigate its impact.

You must know the high-risk sites/branch offices/companies and the specific priority risks that exist in each.

At this point, you must allocate responsibility for each priority risk or aggregated risk category to a specific person/unit.

3. Gradual roll-out of concrete risk assessments

Companies must gradually roll out the procedure for identifying, weighting and prioritizing risks outlined in Step 2 to all companies/branch offices/sites, not only those with increased risk exposure.

Challenges

The implementation of the German Supply Chain Act has already led to significant progress in addressing human rights and environmental violations within supply chains. Companies are increasingly establishing due diligence processes, enhancing transparency, and becoming more accountable for their suppliers' practices. Open complaints mechanisms have also given a voice to potential victims, requiring companies to respond to notifications received from those affected.

However, despite these advancements, companies still face several challenges in fully complying with the Act's requirements:

Complexity and transparency in supply chains

Modern supply chains are intricate and multi-layered, and companies often grapple with limited visibility beyond their direct suppliers, as each additional tier adds complexity and potential opacity. This obscurity makes it difficult to track human rights and environmental risks effectively, especially among indirect suppliers where direct oversight is minimal.

Additionally, acquiring reliable data from suppliers, particularly those deep within the supply chain, poses a significant challenge, as information reliability diminishes with distance and reluctance from suppliers to disclose details exacerbates the issue.

Risk prioritization challenges

The challenge lies in balancing local-specific risks with broader industry norms, as risks vary significantly across different regions and industries. A global corporation may face distinct human rights issues in South Asia compared to environmental concerns in South America, necessitating a flexible yet consistent approach to risk assessment.

Moreover, the dynamic nature of risk factors requires continuous monitoring and swift adaptation to new information. Subjectivity in assessing the likelihood and severity of risks further complicates prioritization, requiring clear, transparent, and importantly, well documented criteria to ensure consistency across various contexts.

Systematic documentation and accountability

Effective risk management mandates comprehensive documentation and clear assignment of responsibilities, yet this is easier said than done. Creating a detailed risk inventory that captures every identified risk, responsible individual, and corresponding preventive and remedial measures is a daunting task. Large organizations, in particular, struggle with integrating risk data from multiple sources into a central system, ensuring completeness and accuracy.

Furthermore, allocating responsibility for specific risks to individuals or units across diverse operations can be challenging. Overlapping duties, staff changes, and ambiguity in risk categorization often cloud the clarity of roles.

Turning prioritization into prevention

LkSG differs from traditional third-party risk management, addressing risks originating from the company's supply chain that can affect broader environmental and social outcomes. This "inside-out" perspective necessitates specific software and a separate risk management framework designed to evaluate the environmental and social impacts of third parties. Companies need separate assessment frameworks distinct from those used in regular supply chain risk management.

SAI360's unified approach to risk management

Unified risk view

SAI360 centralizes all vendor information into a single, accessible platform, transforming fragmented data into a cohesive risk profile. This unified repository integrates records from internal systems, external feeds, and third-party documentation, ensuring no supplier slips through the cracks. Centralization not only enhances transparency but also supports thorough, prioritized risk assessments, helping firms spot and manage risks effectively throughout the entire supply chain.

Supplier engagement and evaluation

SAI360 provides tools for ongoing engagement with suppliers to ensure that they not only meet initial compliance standards but also maintain them consistently. It facilitates regular assessments and audits of suppliers' practices, encouraging continuous improvement and adherence to established ethical and environmental standards. This ongoing evaluation helps in managing supplier risk effectively and ensures that suppliers' compliance efforts are demonstrably effective.

Robust audit trails

The platform's capabilities include creating and managing audit-proof documentation that tracks compliance activities, supplier assessments, and corrective actions taken. This robust documentation serves as evidence of compliance, which is crucial for reporting to regulatory bodies under the LkSG. By maintaining detailed records of compliance measures and their outcomes, organizations can demonstrate their commitment to ethical supply chain practices and regulatory adherence.

SAI360 and the Path to Compliance with the EU Supply Chain Act

The European Commission more broadly has recognized the need for a more coordinated approach to supplier due diligence across the EU. The Corporate Sustainability Due Diligence Directive (CSDDD) represents a marked step forward in requiring companies to identify, prevent, and mitigate actual and potential impacts of their activities on the environment and human rights. Much like LkSG, the directive extends to their operations, subsidiaries, and entities within their value chains.

The CSDDD mandates the development and implementation of prevention action plans, contractual assurances from direct business partners, and subsequent compliance verification. Although the Directive does not come into force until 2025, companies, particularly those in financial services, can benefit from aligning their practices with the CSDDD's trajectory in anticipation of mandatory actions.

In this context, SAI360 provides a comprehensive solution for ensuring compliance with both current and upcoming regulations. By integrating risk management and due diligence processes, SAI360 helps firms comply with the German Supply Chain Act and prepares them for future EU regulations like the CSDDD. This single solution enhances transparency, accountability, and sustainability across operations and value chains

FINAL THOUGHTS

Effective risk analysis under LkSG starts with data, and the predominant challenge is rooted in the need to broaden the view beyond your own business area to that of your third and fourth parties. The sheer volume, complexity and opacity of certain data necessitates the use of sophisticated tools to integrate, centralize and analyze information to provide an integrated, 360-degree view of your risk posture. It's under these circumstances that GRC solutions thrive, facilitating thorough, standardized and well-documented risk analyses across your organization and its entire supply chain.

As BAFA audits approach in 2024, firms' risk analysis procedures will be scrutinized. These audits will demand evidence that firms have taken a data-driven approach to effectively prioritize risks and plan remediation accordingly. Managing risk across the entire supply chain without integrated technology is impractical; therefore, leveraging a solution like SAI360 becomes indispensable. By centralizing risk data and employing sophisticated tools for risk prioritization and management, firms can not only comply with regulatory demands but also proactively mitigate risks, thus laying a solid foundation for effective risk management and mitigation throughout their operations.

Interested in learning more about how SAI360 helps companies comply with the German Supply Chain Act and prepares them for future EU regulations?

Request a demo.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360
RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.

174250 0824