Federal Ministry
for Economic Cooperation
and Development

Partners in
Transformation
Helpdesk Business
and Human Rights

Practical Guide: Supporting Due Diligence with IT Tools and Software Solutions

Michaela Streibelt, Dr. Jana Heinze and Malte Drewes

Content

Introduction: Potentials and Limits of Due Diligence Support with Digital Tools

Companies face the challenge of effectively integrating human rights and environmental due diligence obligations into their processes and identifying risks and violations early on. IT-tools and software solutions offer support by optimising processes, systematically recording data, and facilitating the analysis of complex supply networks.

However – despite their promises – digital solutions also present challenges. The data collected is often incomplete or based on self-reporting, making it difficult to obtain a realistic picture of the actual risks. There is also a risk that companies will rely too heavily on technical solutions, neglect their management responsibility, and overlook direct dialogue with stakeholders – especially those potentially affected. This can result in overlooking important information on human rights and environmental risks and violations that are not captured by software tools.

Other challenges include the fact that companies may not fully understand the evaluation methodology of the IT tools. Furthermore, many applications are not interoperable, meaning that they cannot be easily integrated into the company's own processes. Finally, the cost and effort required to implement many of these tools can pose a hurdle, especially for smaller companies. It is often difficult for these companies to provide the necessary resources for a sustainable digital transformation. This also applies to smaller companies that are integrated in their customers' digital tools.

For these reasons, digital solutions should not be seen as a panacea. Rather, they should be seen as complementary instruments in the due diligence process, which only realise their full value if they are combined with a sound human rights and environmental analysis of their own and a long-term commitment to the rights of those affected. Only in this way can the effectiveness of these solutions be maximized and the constructive perception of obligations by companies be ensured.

This practical guide sheds light on current developments in the field of digital tools for human rights and environmental due diligence, presents use cases and discusses challenges and open questions in dealing with IT tools. To this end, we have addressed the topic in two workshops with companies and civil society organisations. The results of these workshops are summarised in this practical guide to help companies select and use IT tools. Please note: This guide does not describe or evaluate individual IT tool providers.

1. Introduction: Functions of IT Tools

There are many different IT tools to support due diligence processes and correspondingly many functionalities and methods that differ in the details. IT tools, IT solutions or software solutions in this context refer to IT programmes that support companies in the human rights and environmental due diligence process. Tools can be used in practice, for example, for data collection and management, communication with suppliers, and reporting to the relevant authorities. In detail, the various IT tools can partially support companies with:

Risk analysis

Preventive and remedial measures

Complaints procedures

Documentation

Reporting

The aim of many IT tools is to collect and manage information and utilise it for the implementation of due diligence processes. Typical fields of application include, in particular, support in the context of risk analysis (e.g. media screening, analysis of publicly available data sources), supplier management (e.g. supplier profile, questionnaires, specific interventions) or in the documentation and derivation of preventive and remedial measures in cooperation with suppliers (e.g. training, codes of conduct). Importantly, the use of digital tools does not absolve companies from their own due diligence responsibilities.

Overall, the workshops highlighted a wide range of different applications. IT tools differ significantly in terms of both their quality and possible use cases. As a result, it is common practice for some companies to use multiple tools simultaneously in order to address different use cases or meet certain customer requirements. However, effectively integrating digital tools into existing company processes remains a major challenge. In this context, the lack of interoperability was repeatedly emphasised.

BAFA Explanations on the Use of Tools

The BAFA guidance on standards, audits and certifications[1] points out that software solutions rely on their data being validated in order to justify and maintain the trust placed in them. If these tools use report templates, the significance of the results depends on the processed (verified) information. For example, self-disclosures by companies are not independently verified, which can limit their informative value. BAFA also points out that the origin of the data and the methodology for risk assessment are not always fully transparent and comprehensible. According to BAFA, risk screening tools can have difficulties mapping deeper supply chain levels appropriately. One of the reasons for this is that relevant data is missing or not all suppliers worldwide have the necessary technical and human resources. According to the BAFA guidance, it is also challenging to record human rights and environmental risks in informal sectors.

BAFA emphasises that there is sometimes an excessive dependence ('overreliance') on such systems: Companies rely too heavily on the information provided without taking their own measures to analyse and identify risks. This can lead to risks being insufficiently recognised and make effective risk management more difficult. In addition, relying solely on IT tools also leads to incorrect implementation of the law and additional work if the tool does not cover the requirements of the law.

According to BAFA, it is therefore essential that both the mode of operation and the information processed must be as transparent and verifiable as possible – similar to what is required for standards, audits, and certifications. When integrating digital tools into the risk analysis, companies should therefore ensure that they do not blindly rely on the data and evaluations provided, but instead take a risk-based approach and first check on their own responsibility whether and which tools are suitable for implementing the law.

Digital solutions are also often costly and require specific expertise that is not always available within companies. In addition, there is also a lack of standardisation and clear quality criteria for software solution providers. The large number of IT solutions results in incompatible data formats and evaluation methods, making it difficult to compare and utilise the data efficiently. In summary, technical and financial hurdles remain a significant barrier, particularly for small and medium-sized enterprises (SMEs).

[1] https://www.bafa.de/DE/Lieferketten/Handreichungen/handreichungen_node.html, Page 17. last accessed 26 June 2025.

Risk Analysis

Tools allow companies to identify human rights and environmental risks in a structured way, providing an overview of which topics require more in-depth analysis. By using databases, risk mapping software, or automated analysis tools, companies can aggregate and evaluate large volumes of data from various sources, enhancing the transparency and comparability of risks. This helps companies gain valuable insights and adopt a more focused and strategic approach.

Automated screening tools, AI-supported analyses, and risk rating systems can support the risk analysis process by collecting relevant data from multiple sources and identifying potential risks at an early stage. By using software, companies can generate accurate data on working conditions, environmental protection, and other aspects and present it in a clear and accessible way.
As part of data analysis, specific mapping tools make it possible to geographically localize human rights and environmental risks and to pinpoint high-risk regions or sectors. Databases containing country and sector risk profiles enable a fact-based assessment of challenges in specific regions or industries. Depending on the scope and functionality of the software, digital solutions can therefore significantly enhance transparency regarding supplier structures and help identify critical areas in the supply chain.

However, many company representatives report reaching their limits when using tools for analysis, prioritization, and risk assessment. It was emphasized in the workshops that qualitative assessments by the company are often still necessary. Many tools primarily focus on the direct supplier level (tier 1) and only rarely cover the deeper levels of the supply chain, meaning that critical aspects of risk analysis cannot be addressed through digital tools alone. In addition, there are risks and violations in global supply chains that cannot be detected by IT solutions and therefore cannot be included in the risk analysis—particularly in informal sectors.

Preventive and Remedial Measures

There are also various use cases for tools in the implementation phase of measures. For example, tools are used to verify compliance with standards at the supplier level, to meet regulatory requirements, or to store codes of conduct, certifications, and audit-relevant documents. An additional benefit is the ability to provide information in multiple languages (e.g. questionnaires or training materials).

However, the use of such tools remains limited, as the implementation of measures often requires tailored, context-specific solutions, direct engagement with affected stakeholders, and practical adjustments—aspects that can only be partially or not at all addressed by digital tools.

Training and Sensitisation

E-learning tools and interactive training platforms can help raise employees' awareness of human rights and environmental risks.

However, the question remains whether the intended target groups are actually being reached—particularly because many IT applications primarily focus on direct suppliers, thereby overlooking significant portions of the supply chain that should be addressed through a risk-based approach. Some companies reported using these tools in this context, but also emphasized the importance of complementing them with additional measures.

Complaints Procedure

Digital reporting channels, apps, or chatbots can provide potentially affected individuals with low-threshold ways to make contact. Anonymous whistleblower systems with multilingual support increase both accessibility and safety for those affected. It was emphasized during the workshop that initial approaches were being piloted, but these had not yet been implemented on a broad scale.

Monitoring and Documentation

In principle, software solutions enable companies to systematically document human rights and environmental risks and violations, as well as related measures and progress, and to automatically generate reports. Digital solutions can therefore be effectively used for documentation and compliance management. Digital dashboards and tracking tools can support the monitoring of progress in the implementation of measures.

However, some company representatives noted certain limitations, as the scoring would sometimes change (e.g. when suppliers upload documents) without the user being informed or able to understand the evaluation. In some cases, failure to answer questions can also result in a risk classification.

Conclusion

Overall, tools can and are used at various points in the due diligence process. However, they must be regularly assessed by the company in terms of quality, benefits, and scope, and supplemented by internal measures.

Most company representatives identified the greatest added value in the use of tools in risk analysis. In the next section, we take a closer look at the possible applications for this step of the due diligence process.

2. Spotlight Risk Analysis

Many IT applications start with risk analysis and can, in some cases, significantly simplify this process for companies. In the following chapter, companies will first be introduced to the key requirements arising from the German Supply Chain Due Diligence Act (LkSG) in relation to risk analysis. Following an overview of the opportunities and challenges associated with digital tools in this context, as well as insights into the involvement of potentially affected stakeholders, the chapter presents a step-by-step guide outlining what needs to be considered when integrating such tools into the company's risk management process.

Requirements for the Risk Analysis

The annual and ad hoc risk analysis of the company's own operations and direct suppliers (Section 5 LkSG), as well as the ad hoc risk analysis of indirect suppliers (Sections 5(4) and 9(3) LkSG), constitutes a core element of risk management under the LkSG.
Its purpose is to identify, assess, and prioritise human rights and environmental risks and violations within the company's operations and across the supply chain. This analysis serves as a preparatory step for defining and implementing preventive and remedial measures.
The LkSG requires a risk-appropriate analysis, thereby embedding a risk-based approach. It does not require companies to analyse all (direct) suppliers annually. Instead, companies are expected to apply a risk-based approach and may only need to review a selection of suppliers—with varying degrees of scrutiny depending on the risk level.

Mapping: The LkSG does not specify the risk analysis process in detail. However, it is recommended to divide the process into several clear steps. One proven approach is to begin with a mapping exercise to gain an overview of the company's own suppliers, supply chains and networks, potential risk areas, and relevant stakeholder groups. This can be done, for example, using a heat map. If the supplier base is extensive, companies should use the heat map as a basis for selecting which suppliers to examine more closely in the subsequent steps of the risk analysis.

abstract and concrete Risk Analysis: The next step involves conducting an abstract risk analysis to obtain an initial overview of potential risk areas. To do this, companies consult generally accessible sources such as media reports, publications from non-governmental organisations (NGOs), government agencies, and academic literature. These findings form the basis for a more concrete risk analysis, which aims to validate the information in relation to specific suppliers, supply chains, or networks. Common tools used at this stage include self-assessment questionnaires and audits. However, it should be noted that the informative value of questionnaires and pre-announced audits is limited.[2]

Stakeholders: Including stakeholders is a further key step in the risk analysis under the LkSG. This obligation derives from the requirement to appropriately consider the interests of potentially affected parties, as outlined in Section 4(4) of the LkSG. Involving those potentially affected is especially important, as they can provide direct insight into on-the-ground realities — such as working hours, wages, and occupational health and safety. In cases where suppliers may withhold or distort information, these individuals serve as a critical corrective.

Their perspectives can be included through direct consultation or via legitimate interest groups such as trade unions or NGOs.[3]

Opportunities and Challenges of IT Tools in Risk Analysis

IT tools make it easier for companies to implement human rights and environmental due diligence, particularly by improving efficiency and scalability. They enable efficient, systematic, and automated collection of large volumes of data from complex supply chains. The use of tools can be particularly worthwhile for companies with a large number of suppliers. Some companies perceive added value in using tools to identify potential human rights and environmental risks and violations at an early stage, enabling them to allocate resources more strategically, particularly to fulfil due diligence obligations in extensive supply networks.

Digital solutions potentially increase transparency and in some cases facilitate the tracking and traceability of products and raw materials in complex supply chains. However, such tools generally only provide reliable data for formalised supply chain activities, and in many cases, this is limited to direct suppliers (tier 1).

A key problem here is the limited availability and quality of data. Many companies only have limited information about the deeper stages of their supply chains, and the data they receive via IT tools is often (still) incomplete or outdated. Important areas of global supply chains—such as small-scale mining, agricultural field labour, or home-based work—are often not sufficiently covered by IT tools. However, as the risks in many industries often lie specifically in the deeper tiers of the supply chain, software solutions can only serve as one component of the overall risk analysis.

[2] See https://www.bafa.de/EN/Supply_Chain_Act/Risk_Analysis/risk_analysis_node.html, last accessed 26 June 2025.

[3] See „BAFA FAQ on the risk-based approach" https://www.bafa.de/SharedDocs/Downloads/EN/Supply_Chain_Act/faq_risk_based_approach.html, last accessed 26 June 2025.

In addition, some company representatives also noted deficiencies in the reliability and quality of the data. Examples of this include the fact that the structure is not always based on NACE codes, that news monitoring is not subsequently checked for plausibility, and that publicly funded sources (e.g. reports from governments, the United Nations, or NGOs) are not always included to a sufficient extent. Data collected specifically via the tools—for example, through questionnaires—does not always provide the necessary information for the risk analysis.

Many tools primarily supply raw data. This data must then be integrated by the company into its internal processes. However, some companies also report that this is often not possible without additional effort (keyword: lack of interoperability). Companies must also take data protection and cybersecurity into account. The processing of sensitive supply chain information harbours risks, especially when data is managed by third parties or platform providers.

Integration of certain Tool Functions into your own Risk Analysis – Step-by-Step Analysis

The following steps can help you to support your own risk analysis with digital solutions.

STEP 1 – DEFINITION OF THE RISK ANALYSIS PROCESS

Firstly, companies should define their analysis process. This step involves identifying relevant risks and violations, assessing and prioritising them, and defining responsibilities. A structured approach helps to systematically record relevant human rights and environmental risks and violations, set priorities, and assign responsibilities. It is important to define a clear objective before using a tool—in other words, to be clear about which specific risks and violations are to be identified and which decisions will be based on the analysis. The risk analysis should not be viewed in isolation, but should be embedded in the company's overall due diligence strategy.

STEP 2 – CRITICALLY ANALYSE THE FUNCTIONS AND DATA OF IT TOOLS

The next step is to analyse which data and functions the corresponding IT tool actually provides or could provide. Companies should scrutinise the extent to which this information is sufficient for their specific requirements and where additional input may be necessary. Many IT tools that support risk analysis currently focus, for example, on providing a heat map and sending and following up on self-assessment questionnaires. In practice, this means that suppliers complete a questionnaire at the company's request after setting up an account. The efforts and costs incurred by suppliers include the lack of interoperability, which forces them to repeatedly complete questionnaires that are similar but differ in detail.[4]

[4] This problem also exists when several buying companies subject to the LkSG each submit their own questionnaires to their suppliers for self-assessment. See https://www.bafa.de/SharedDocs/Downloads/EN/Supply_Chain_Act/guidance_cooperation_supply_chain.pdf?__blob=publicationFile&v=6, last accessed 26 June 2025.

Info Box: Challenges in including the Perspective of those potentially Affected

In the dialogue with NGOs, it was emphasised that the perspective of those potentially affected by digital tools has so far only been taken into account to a limited extent. Many solutions focused on risk assessments based on publicly available data, certifications or self-reporting by companies.

Participatory approaches that directly involve those affected are still rare, although initial progress such as complaint mechanisms via apps and participatory monitoring approaches are recognisable.

A major obstacle is the lack of access to digital technologies, language and cultural barriers as well as a lack of trust in digital systems, especially in rural or resource-poor regions. Data protection and anonymity are therefore crucial to encourage participation.

Integrating feedback into companies' due diligence processes remains a challenge, as the necessary structures and processes for systematically involving potentially affected parties are often lacking.

- A hybrid approach that combines digital and analogue formats could overcome these barriers and also reach people without digital skills.
- Cooperation with local organisations such as NGOs and trade unions can build trust and increase acceptance.
- In addition, those affected should be actively involved in the design of the tools in order to make them needs-based and accessible.
- Legal requirements or incentives could encourage companies to make greater use of participative digital solutions.
- Ultimately, companies must ensure that data protection is maintained in order to prevent repression. Trust is created through long-term commitment and continuous engagement with the causes of the problems.

Overall, the involvement of stakeholders in digital tools offers great potential, but requires a holistic approach that addresses technological, social, and ethical challenges.

Bureaucratic and often less effective efforts also arise when tools pursue so-called „watering can approaches"—i.e. tools automatically send questionnaires to all direct contractual partners entered into the system. Many tools allow for the entry of the full list of vendors, including authorities such as local tax offices. In some cases, documents such as audit reports or internal policies can be uploaded, although only a few providers currently verify their content. In some instances, this leads suppliers to develop policies that improve scoring, even though the topics covered may not be relevant or actually implemented by the company. An approach based solely on standardised questionnaires is also problematic, as it leaves potential gaps in the risk analysis. In addition to direct suppliers, companies must also consider their own business operations and, where necessary, indirect suppliers.

Companies should therefore critically examine what data the IT tool provides, how current and reliable it is, and where further information is needed.

BAFA also emphasises the importance of a risk-based approach, the inclusion of the data subject's perspective, coverage of the full supply chain, and technical aspects such as interoperability (see info box page 5). In this context, the company should also examine whether the origin and quality of the data are accessible. The design and logic of the underlying algorithm used in the respective software solution must be transparent and comprehensible to users.

The following questions provide guidance when reviewing the functionality of tools as part of the risk analysis.

Questions for Analyzing the Functions of IT Tools for the Risk Analysis

- ✓ Does the tool follow a **risk-based approach**?
- ✓ Which **human rights and environmental risks** are in focus (e.g. child labor, forced labor, discrimination)?
- ✓ Does the tool reach the **right addressees**?
- ✓ Are **all relevant stages** of the supply chain and regions mapped (including the company's own operations and the deep supply chain)?
- ✓ What is the **quality** of the questions asked?

- Does the tool take into account the **different information requirements** in the deep supply chain?
- Is the **evaluation logic** transparent and comprehensible?
- Can **own considerations** be included in the analysis?
- What **decisions** should be made on the basis of the analysis (e.g. adaptation of procurement, training for suppliers, audits)?

STEP 3 – IDENTIFY INFORMATION GAPS

As explained in Step 1, companies should specifically examine what data the IT tool provides, how up to date and reliable it is, and where additional information may be needed.

Some providers currently rely on standardised questionnaires that may have limited relevance in specific cases. For example, questionnaires are used that have converted the individual protected legal positions of the LkSG into yes/no questions such as "Do you employ children?" or "Do you comply with all laws?"

Such questions are sometimes unsuitable for drawing meaningful conclusions about risks and violations and may simply be redundant for companies operating in industries or countries with a low risk of human rights violations (e.g. child labour at a food importer in Germany). Such approaches may also result in an excessive focus on tier 1 suppliers, while high-risk upstream suppliers remain hidden. If, for example, a chocolate importer based in Germany states that child labour and forced labour are not issues in its own operations, there is a risk that these issues will go undetected in relation to upstream suppliers in producing countries. Such an approach creates unnecessary bureaucracy and is ineffective, as it is not based on actual risk.

There is also a risk that the right target groups are not being reached. Questionnaires are usually completed by the supplier's management, not by the workforce, which means the interests of those affected are only reflected to a limited extent.

While some questions should indeed be directed at management (e.g. regarding certificates, policies, or management systems), questions concerning the situation of rights holders (e.g. working hours or worker participation) should also be addressed to those potentially affected or their legitimate representatives.

STEP 4 – DEVELOP SUPPLEMENTARY MEASURES

If the tool used does not provide all the relevant information (see challenges above), additional actions are necessary to ensure a comprehensive and well-founded risk analysis.

These supplementary measures include, for example:

1. **Targeted, risk-based questionnaires** for high-risk suppliers to gain deeper insights into their labour practices and potential human rights risks.

2. **Company-specific or supply chain-specific questionnaires** to collect tailored information that goes beyond standardised questions.

3. **On-site visits and audits** for high-risk suppliers to gain an overview of the situation in the factory or in the field, and to guide the implementation of measures along the supply chain.

4. **Stakeholder consultations** to integrate different perspectives. Dialogue with NGOs, trade unions, and other relevant actors provides valuable, practical insights for a well-founded risk analysis.

Depending on the context, very different preventive and remedial measures may be necessary—depending on their appropriateness and effectiveness. In this respect, the list of supplementary measures should be regarded as a suggestion, not as an exhaustive list.

General Information on the Use of Tools in the Due Diligence Process

As described at the beginning, digital tools are also used in relation to other due diligence obligations. The following tips will help you to use them appropriately and effectively.

Including Your Own Expertise in a Targeted Manner

Digital tools offer valuable support, but they must not replace human judgment. Particular caution is warranted when software providers make very generous compliance promises. It is crucial that companies apply their own expertise—especially when prioritising risks and violations and developing appropriate measures. A purely automated analysis can overlook important nuances that can only be considered through the expert assessment of experienced staff—for example, from the purchasing department. This is especially important when determining which risks and violations are considered particularly serious and which measures are most effective. Companies should therefore actively involve the relevant specialist departments and colleagues in the use of software solutions and continuously refine their application rather than blindly relying on the tool.

Seamless Integration into Existing Processes and Observing Technical Limits

IT solutions should not be viewed in isolation or as stand-alone solutions within a company. Instead, they must be meaningfully integrated into existing risk management and decision-making processes. This is the only way to fully exploit the potential of the applications. Digital solutions should therefore become an integral component of the risk management process to ensure that all relevant data and insights are used systematically.

Continuous Review and Optimisation

The use of digital solutions must be evaluated regularly to ensure that they continue to meet changing requirements and framework conditions. A continuous review makes it possible to identify weaknesses at an early stage and make adjustments if necessary. The rapidly evolving technological landscape and new legal requirements necessitate ongoing adjustments to the tools used in order to ensure their long-term effectiveness. In addition, ongoing optimisation helps to maximise the benefits of digital solutions and enhance the accuracy of risk analysis.

Further Information

BAFA Guidance Risk Analysis:

This ↗ Guidance from the Federal Office of Economics and Export Control (BAFA) provides companies with instructions on how to carry out risk analyses within the framework of the Supply Chain Duties Act (LkSG).

BAFA Guidance Standards (German only):

This BAFA ↗ Guidance provides specific guidance on the selection and use of standards, audits and certifications as instruments for fulfilling due diligence obligations under the LkSG.

BAFA and Helpdesk Guidance Collaboration in the Supply Chain:

This ↗ Guidance produced by the BAFA together with the Helpdesk for Business and Human Rights, shows what obligated companies can and cannot ask their suppliers to do under the LkSG. It also contains recommendations for constructive cooperation.

BAFA FAQ on the risk-based approach:

The BAFA has published ↗ questions and answers with clarifications on the risk-based approach to risk analysis and cooperation in the supply chain.

CSR Risk Check:

The CSR Risk Check is an ↗ online tool that helps companies to assess the local human rights situation as well as environmental, social and governance issues.

BMWK/BMAS dialogue series fair supply chains (German only):

The Federal Ministry of Labor and Social Affairs, together with the Federal Ministry for Economic Affairs and Climate Protection and the Helpdesk on Business and Human Rights, has launched the #Faire Lieferketten ↗ dialogue series for companies and interested business associations.

Imprint

Helpdesk on Business and Human Rights
(implemented by DEG Impulse with support from GIZ)

DEG Impulse gGmbH
Kämmergasse 22
50676 Köln / Germany

E-Mail: kontakt@helpdeskwimr.de
Website: www.helpdeskwimr.de

Follow us on social media and stay informed about current developments on the topic of business and human rights:

Helpdesk Wirtschaft und Menschenrechte

Status: 26 June 2025