FERMA
Federation of European Risk Management Associations

5 September 2022

Guide to Using a Risk-Based Approach to Implement Value Chain Due Diligence

FERMA FOCUS
SUSTAINABILITY

A risk-based approach to value chain due diligence is more likely to achieve good results than an exhaustive approach. Companies need to identify and remedy the most likely problems and not miss them in noise.

The Federation of European Risk Management Associations (FERMA) strongly supports the European Commission's ambitions for the Corporate Sustainability Due Diligence Directive (CSDDD), but we believe there would be practical difficulties implementing the directive requirements as currently proposed (as we have mentioned in our position paper).

We, therefore, recommend that the European Parliament integrates a risk-based approach to value chain due diligence both within the recitals and throughout Articles 3-11 at the least.

In this document, FERMA presents a simplified illustration of a risk-based approach to conducting value chain due diligence as part of the CSDDD. This is based on the expertise of our members.

Our illustration focusses on suppliers and subcontractors, but the same consideration and approach is easily applied to other third parties, such as those in partnerships.

Furthermore, using a risk-based approach to value chain due diligence will be useful for corporates in their overall approach to managing sustainability risks.

Also, companies in scope of the Corporate Sustainability Reporting Directive (CSRD) will have to perform double materiality reporting.

This implies that companies will have to employ a risk-based approach to reporting, even though it may differ to the approach presented below.

Key steps in a risk-based approach

Identify high risk third parties using defined criteria and method.

Create an operational roadmap for the application of human rights and environmental due diligence to the identified third parties.

Conduct the due diligence on these high-risk third parties to analyse the maturity level of their sustainability risk management.

Define a risk management strategy to apply to all categories of third parties.

The following illustration of a risk-based approach to value chain due diligence derives from the established Enterprise Risk Management (ERM) methodology and draws on good practices applied in some of the most mature companies regarding risk management.

This approach combines the use of ERM, by which the company identifies the sustainability risk of related third parties. Based on that assessment, the company performs deeper analysis, validated against the information collected from the third parties.

STEP 1 – Identify high risk third parties

Analyse the third parties cooperating with the company considering their potential to expose the company to the risk of adverse environmental and human rights *and* business impacts.

Rank the companies by high, medium or low categories of risk according to **the potential severity of adverse impact**[1].

For suppliers, including tier 1 sub-contractors, factors are likely to include:

- ✓ **Type of purchase:** direct, indirect, or external services/advisory.
- ✓ **Type of material/service**: materials with high environmental impact or from industries with human rights issues or services like payroll management
- ✓ **Geographical area** based on international indices, such as Human Rights Watch, or the UN Universal Human Rights Index
- ✓ **Business dependence**: single source or >50% of group purchases, high production interdependence or multiple suppliers.
- ✓ **Probity of the supplier or sub-contractor**: relevant standards adopted by supplier or negative reputation.

Using this methodology the risk manager determines a final RISK EVALUATION, based on the importance (weighting) of the categories and ranks the parties as High, Medium or Low risk. They then create a register of the high risk third parties.

STEP 2 – Conduct Due Diligence on High-Risk Third Parties

The risk manager creates an operational roadmap for the application of human rights and environmental due diligence to the identified third parties.

This will allow an analysis of the maturity level of the sustainability risk management system of these third parties, and the associated risk exposure.

Using completed self-assessment questionnaires, supporting documentation and in some cases onsite audits, the risk manager will assign a RISK EVALUATION to the third party.

STEP 3 – Third Party Risk Management Strategy

Companies will define the relevant strategy to be applied to each identified category of parties.

They will integrate into the company's business processes (for instance supplier selection) the sustainability due diligence results and the overall evaluation of third party, as well as other business evaluations (financial evaluation, for example).

Based on the RISK EVALUATION assigned to the self-assessment questionnaire, the Company can then decide to:

a. Low risk parties: continue with the collaboration.
b. Medium risk parties: require a defined action plan for improvements over the medium term (e.g., 6 months/1 year).
c. High risk parties, require an immediate remediation plan (e.g., by 3 months) or consent from Top Management to continue cooperation (for example if it is not possible to find an alternative supplier) or end the relationship.

The above process should be explicitly included into the company's Procurement Procedure.

FERMA's illustration is intended to start a discussion on what risk-based value chain due diligence might look like. Thank you for your consideration.

---

[1] *In reference to Articles 3 (b) and 3 (c) of the proposal*