Background note on Regulatory Developments concerning Due Diligence for Responsible Business Conduct

Translating a risk-based due diligence approach into law

Please cite as: OECD (2022), *Translating a risk-based due diligence approach into law: Background note on Regulatory Developments concerning Due Diligence for Responsible Business Conduct*

https://mneguidelines.oecd.org/translating-a-risk-based-due-diligence-approach-into-law.pdf

This document is part of a series of notes considering issues related to the design and implementation of mandatory environmental and social due diligence legislation related to OECD standards on responsible business conduct (RBC).

It contributes to the OECD Due Diligence Policy Hub which presents technical papers, event information, tools and other resources to help policy makers improve the design of legislation and regulation on due diligence for RBC. The hub is managed by the OECD Centre for RBC with a view to helping governments leverage the wide-ranging policy measures at their disposal to promote RBC.

Find out more at http://mneguidelines.oecd.org/due-diligence-policy-hub.htm

Foreword

This document is part of a series of background notes considering issues related to the design and implementation of mandatory environmental and social due diligence legislation related to the OECD Guidelines for Multinational Enterprises and OECD Due Diligence Guidance for Responsible Business Conduct (RBC). It considers key principles and elements of the risk-based approach under the OECD RBC due diligence standards and presents options for translating these into mandatory requirements, based on examples from existing risk-based legislation in other contexts.

The document contributes to the OECD Due Diligence Policy Hub which presents technical papers, event information, tools and other resources to help policy makers improve the design of legislation and regulation on due diligence for RBC. The hub is managed by the OECD Centre for Responsible Business Conduct with a view to helping governments leverage the wide-ranging policy measures at their disposal to promote implementation of RBC.

This report was prepared by Emily Norton and Barbara Bijelic from the OECD Centre for Responsible Business Conduct. The report was developed under the direction of Allan Jorgensen, Head of the OECD Centre for Responsible Business Conduct. Communications support was provided by Roxana Glavanov.

Find out more at https://mneguidelines.oecd.org/mneguidelines/ and http://mneguidelines.oecd.org/due-diligence-policy-hub.htm

Introduction

Growing momentum around mandatory human rights and environmental due diligence has led to questions about how to translate the "risk-based approach" set out in international standards into legal requirements in a manner that provides sufficient legal certainty as well as flexibility for companies. The OECD Guidelines for Multinational Enterprises (MNE Guidelines) and OECD Due Diligence Guidance for Responsible Business Conduct (RBC) set out the expectation that enterprises carry out *risk-based* due diligence. This means prioritising their most severe risks and impacts—regardless of where they sit in the value chain. It also involves tailoring due diligence to the nature of risks companies face in practice.

In designing RBC due diligence obligations for companies, governments can draw from examples of risk-based legislation in other contexts. Risk-based frameworks are increasingly seen as a necessary part of "better regulation", and have long been used by regulators and legislators to help define the risk identification, prevention and mitigation measures entities should take in the context of risks to society and the environment.[1] A risk-based approach is central to legislation concerning anti-money laundering and counter-terrorist financing, bribery and corruption, health and safety, food and product safety, data protection and anti-slavery, and—to varying degrees—existing human rights and environmental due diligence legislation.

Although existing laws vary in scope and focus, risk-based approaches share the general principle that companies' risk management should a) target those areas of the business where risks are greatest and, on that basis, prioritise the highest risk business partners b) be proportionate and tailored to the degree and nature of risk that individual companies face.

This background note considers key principles and elements of the risk-based approach under OECD RBC due diligence standards and presents options for translating these into mandatory requirements, based on examples from existing risk-based legislation[2].

Section 1 explains key principles and elements of risk-based due diligence under international RBC due diligence standards. **Section 2** presents options for translating a risk-based due diligence approach into law. Specifically, Section 2 discusses options for ensuring that, consistent with international standards, companies:

1. Prioritise appropriately on the basis of severity and likelihood
2. Put in place credible prioritisation processes
3. Respond appropriately to identified risks and adverse impacts
4. Demonstrate credible prioritisation processes and progress against outcome-based targets
5. Are not unreasonably sanctioned for adverse impacts that materialise in relation to risks they credibly deprioritise

1. Key principles and elements of risk-based due diligence under international due diligence standards

1.1. What is the risk-based approach?

Under OECD RBC due diligence standards[3], enterprises are expected to carry out risk-based due diligence to identify, prevent, mitigate and account for how they address actual and potential adverse impacts to people, society and the planet. As it will often not be possible for enterprises to identify or respond to all risks and adverse impacts related to their activities and business relationships simultaneously and with the same degree of attention, the MNE Guidelines encourage enterprises to prioritise their most severe risks and impacts. In this respect, the MNE Guidelines and OECD Due Diligence Guidance for RBC are aligned with the United Nations Guiding Principles.

The risk-based approach encompasses two "key characteristics" or principles of due diligence (see Box 1). It is an essential part of ensuring that:[4]

- enterprises **prioritise** their most significant adverse impacts on the basis of severity and likelihood of harm and, on that basis, focus their attention and resources on their higher-risk operations and business relationships; and
- enterprises' due diligence measures are sufficiently **tailored** to the nature, severity and likelihood of the specific risks and adverse impacts they identify.

Box 1. The risk-based approach under OECD RBC due diligence standards

The OECD MNE Guidelines state that: "Where enterprises have large numbers of suppliers, they are encouraged to identify general areas where the risk of adverse impacts is most significant and, based on this risk assessment, prioritise suppliers for due diligence" (MNE Guidelines, Chapter II, Commentary, paragraph 16).

The risk-based approach is further elaborated in the OECD Due Diligence Guidance for RBC and encompasses the following "key characteristics" of RBC due diligence:

(a) **The measures an enterprise takes should be commensurate to the severity and likelihood of the adverse impact**. When the likelihood and severity of an adverse impact is high, then due diligence should be more extensive. Due diligence should also be adapted to the **nature** of the adverse impact (e.g. human rights, environment or corruption), which involves tailoring approaches for specific risks and taking into account how these risks affect different groups.

(b) **Where it is not feasible to address all identified impacts at once, an enterprise should prioritise the order in which it takes action based on the severity and likelihood of the adverse impact**. Once the most significant impacts are identified and dealt with, the enterprise should move on to address less significant impacts. Where an enterprise is causing or contributing to an adverse impact on RBC issues, it should always stop the activities that are causing or contributing to the impact and provide for or cooperate in their remediation. The process of prioritisation is also ongoing, and in some instances new or emerging adverse impacts may arise and be prioritised before moving on to less significant impacts.

Source: OECD Due Diligence Guidance for RBC (2018), Overview and Annex, Q3 to Q5, and OECD (2011), Commentary on General Policies, Para 16.

Risk-based due diligence is concerned with making progress on the most significant adverse impacts to people, planet and society. Companies are expected to focus their attention and resources on where they are most urgently needed—not on the basis of other factors, such as where risks and impacts sit in the value chain, the degree of influence or leverage an enterprise has over a particular business partner, or the extent to which the impacts at issue are deemed to be financially material (see Section 1.2 below). This perspective is fundamental to achieving the core objective of RBC due diligence which is to avoid or seek to prevent adverse impacts on people, planet and society. Contextual factors, such as the degree of leverage a company has over a particular business relationship, will impact the actions companies take to address an impact—but not how they prioritise.

The risk-based approach helps to ensure that due diligence is practicable for companies. By allowing companies to prioritise, risk-based due diligence recognises that businesses will not be able to address all the risks and impacts they are connected to across value chains simultaneously. As such, a risk-based approach does not expect companies to identify and respond to every adverse impact, monitor and track every business partner or trace every product. It does not expect perfect results or 100% risk-free value chains and does not penalize companies simply for the presence of risks or adverse impacts in their operations and value chains. Instead, it expects enterprises to prioritise appropriately, target their highest risk operations and business relationships and demonstrate meaningful and measurable progress over time against specific, time-bound targets and indicators.

OECD RBC standards seek to strike a careful balance between specificity and flexibility in how the risk-based approach is operationalised. For example, the OECD Diligence Guidance for RBC and sectoral guidances include specific expectations about the factors that inform prioritisation decisions and the necessary elements for credible prioritisation (Sections 1.2 and 1.3 below). But the risk-based approach also gives companies flexibility to adapt their due diligence to their prioritised (ie. most significant) risks and impacts, recognizing that different types of harms will necessitate different approaches. How a company identifies, tracks and responds to incidents of child labour detected at a particular business relationship will look very different to how it manages health and safety risks or incidents of water contamination.

These key principles reflect standard ways of thinking about risk assessments and prioritisation, with an important difference being that the focus is on the degree of risk to people, society and the planet—not risk to business. Likewise, the flexibility and the degree of discretion given to companies is no different conceptually from other risk-based approaches (see Section 2 of this note).

The flexibility inherent to RBC standards does not, therefore, imply that companies can arbitrarily decide what is and is not important. Instead, OECD RBC standards set important parameters for how and when companies may prioritise. Demonstrating credible prioritisation processes and progress against outcome-oriented targets consistent with the expectations set out in the due diligence framework become critical (Section 1.3 below). These and other elements help to ensure that companies arrive at decisions

about allocating resources and time to particular issues over others in a way that is efficient, effective and aligned with international standards.

The expectation that companies prioritise risks and impacts on the basis of severity and likelihood flows through the entire due diligence process—starting with the company's initial high-level scoping of broad risk issues and, on that basis, the higher-risk operations and business relationships it selects for deeper-dive risk assessments and then how it chooses which site-level impacts to respond to first. It also shapes how companies are expected to track and report on their due diligence. See Box 2 and Annex B.

Box 2. Prioritisation and the OECD 6-step due diligence framework

Enterprises are expected to prioritise according to severity and likelihood across the six-step framework. This Box, together with Annex B, sets out examples of prioritisation *measures* under the OECD MNE Guidelines and Due Diligence Guidance for RBC. It does not provide a comprehensive summary of expectations for ensuring that enterprises' prioritisation *processes* are credible. Examples of prioritisation measures include:

- **Step 1 - Embed RBC into policies and management systems**: Enterprises progressively tailor their RBC due diligence policies and management systems to their most severe and likely risks, as identified and prioritised under Step 2.
- **Step 2 - Identify and assess actual and potential adverse impacts**: Enterprises:
  - Carry out a broad, **high-level scoping exercise** of the enterprise's operations and types of business relationships in order to prioritise actual and potential RBC risk issues (e.g. forced labour, GHG emissions), taking into account "**risk factors**" (Step 2.1).
  - On the basis of the prioritised risk issues, select **individual higher-risk operations and business relationships** for **in-depth mapping and risk assessments** to identify specific site-level adverse impacts. Further prioritisation may be needed among high-risk business relationships (Step 2.2).
  - Reassess impacts at regular intervals to identify new and emerging risks and impacts, and prioritise appropriately.
- **Step 3 - Cease, prevent and mitigate adverse impacts**: Enterprises prioritise specific risks and impacts for action on the basis of severity and likelihood. They move on to address less severe impacts once prioritised impacts have been addressed. Risk prevention and mitigation strategies include appropriate time-bound targets, with a focus on prioritised impacts.
- **Step 4 - Track implementation and results**: Companies carry out ongoing monitoring and track progress on risks and adverse impacts, prioritising those impacts they assessed to be most significant and took action to prevent or mitigate under Step 3.
- **Step 5 - Communicate how impacts are addressed**: Companies report on their prioritised risks and impacts, prioritisation criteria and processes, and actions and outcomes to address priority impacts against targets.
- **Step 6 - Provide for or cooperate in remediation:** Companies participate in remediation for impacts that they cause or contribute to. Legitimate remediation mechanisms and early warning systems allow stakeholders to raise complaints about emerging impacts; these feed into companies' ongoing risk prioritisation.

Note: The OECD Due Diligence Guidance for RBC sets out examples of sectoral, geographic, product and enterprise risk factors that enterprises can consider when prioritising risk issues and individual operations, suppliers and other business relationships under Step 2.1. See below on 'Ensuring credible prioritisation processes'. See OECD sectoral due diligence guidances for more information on sector-specific risks and risk factors.
Source: OECD Due Diligence Guidance for RBC (2018)

1.2. Ensuring appropriate prioritisation criteria: severity and likelihood

The "significance" of a potential or actual adverse impact is defined on the basis of its severity and, for potential adverse impacts that have not yet occurred, the likelihood (or probability) of that impact occurring. Factors such as the degree of leverage or control a company has over a particular business relationship, or risks to the business—are generally not relevant to whether a company *should* prioritise a specific risk or impact. They may, however, impact *how a company responds* to prioritised impacts (see paragraph (d) below).

Severity is not an absolute concept and is context specific; where the risk of a potential impact is most likely and most severe will be specific to the enterprise, its sector and the nature of its business relationships.[5] Severity is determined according to three factors, set out in the OECD Due Diligence Guidance for RBC:

- **Scale:** the *gravity or seriousness* of the potential or actual impact, such as the degree of serious impact on workers' health and safety, degree of waste or chemical generation; or loss of life or severe bodily harm caused,
- **Scope:** the *reach or extent* of the potential or actual impact, for example the number of individuals that are or will be affected, or the extent of environmental damage or other environmental impact**;** and
- **Irremediable character:** its *irreversible nature*, or any limits on the ability to restore the individuals or environment affected to a situation equivalent to their situation before the adverse impact.[6]

This prioritisation criteria represents a shift in how companies traditionally think about how they approach mapping and assessing their business relationships. For example, there can be a tendency among many businesses to focus their attention on direct or Tier 1 business relationships or longer-term partners as they are perceived to be "closer to home" and easier to control, before then moving on to map and evaluate Tier 2 or Tier 3 business relationships. In the context of due diligence regulation, limiting the scope of due diligence expectations to Tier 1 business relationships has also been proposed by some policy makers as an appropriate way to make such expectations implementable and realistic for business.

However, focusing on direct business partners, longer-term relationships, or where companies face greatest risks to the business can lead to companies misallocating scarce resources and time to assessing lower risk actors in the value chain, leaving more severe impacts and higher risk business partners unaddressed. This can be a costly and unnecessarily expansive approach—requiring companies to apply comprehensive due diligence across relevant entities, irrespective of the degree of risk involved. Direct business relationships may often be intermediary buyers, primary product processors, or agents and so may not always the most appropriate target of a company's due diligence. In contrast, a significant adverse impacts may often be "hidden" further down the in supply chains beyond the first tier. For example, research by the OECD has concluded that, globally, between 28 and 43 per cent of the child labour estimated to contribute to exports does so indirectly through upper tiers of the supply chain (such as extraction of raw materials or agriculture).[7] A Tier 1 approach can also create perverse incentives: to avoid proximity to risk or to have control or leverage over, or long-term relationships with, individual business partners.

In some cases a focus on direct business partners or specific tiers, or long-term business partners, may be justified—for example, if the company determines that this is where its most severe impacts are most likely to arise or if those business partners act as a key point of leverage or 'choke point' in the value chain.[8] **However, companies should not prioritise direct or long-term business partners at the expense of more significant and urgent risks that are further removed.**

1.3. Ensuring credible prioritisation processes

Where companies prioritise, it is important not only that they do so based on the factors of severity and likelihood, but also that they put in place credible prioritisation processes. This section discusses the following elements, each of which helps to ensure that companies prioritise appropriately and in line with due diligence standards:

- The role of the scoping exercise and "risk factors" in prioritisation
- The importance of stakeholder engagement
- Ensuring that new and evolving risks feed into prioritisation processes

The role of the scoping exercise and "risk factors" in prioritisation

OECD RBC standards emphasise the importance of enterprises carrying out an initial high-level scoping exercise—across their operations and types of business relationships—to first identify and prioritise their most severe and likely risk issues (such as GHG emissions, water contamination, forced labour or unpaid work) on the basis of "risk factors" (Step 2.1). They are expected to gather information from a range of sources, including relevant expert stakeholders, and consider possible sectoral, geographic, product and enterprise-level risk factors or indicators of potentially higher risk (see Box 3).[9] This reflects risk-based approaches in other context, such as anti-money laundering and counter-terrorist financing (see Section 2.2 of this document).

Box 3. Risk factors under the OECD Due Diligence Guidance for RBC

The OECD Due Diligence Guidance for RBC sets out the following examples of risk factors that enterprises may consider as part of their risk scoping exercise under Step 2.1. These are further elaborated in Annex A.

- **Sector risks** are risks that are prevalent within a sector globally as a result of the characteristics of the sector, its activities, its products and production processes. For example, the extractive sector is often associated with risks related to a large environmental footprint and impacts on local communities. In the garment and footwear sector, risks associated with respect for trade union rights, occupational health and safety and low wages are prevalent, amongst others.
- **Product risks** are risks related to inputs or production processes used in the development or use of specific products. For example, garment products with beading or embroidery hold a higher risk of informal employment and precarious work and phones and computers may contain components that are at risk of being mined from conflict areas.
- **Geographic risks** are conditions in a particular country which may make sector risks more likely. Geographic risk factors can generally be classified as those related to the regulatory framework (e.g. alignment with international conventions), governance (e.g. strength of inspectorates, rule of law, level of corruption), socio-economic context (e.g. poverty and education rates, vulnerability and discrimination of specific populations) and political context (e.g. presence of conflict).
- **Enterprise-level risks** are risks associated with a specific enterprise such as weak governance, a poor history of conduct in relation to respecting human rights, labour rights, anti-corruption standards, environmental standards, or a lack of culture around RBC

Source: OECD Due Diligence Guidance for RBC (2018).

Ensuring that companies take a holistic approach and consider a broad range of contextual risk factors and data sources helps to ensure that companies' prioritisation decisions are, from the very outset, informed and tailored to their own circumstances—based on their relevant sectoral, product, geographic and business partner risks. It helps companies to take a step back and ensure they have credible scoping and prioritisation processes in place *before* selecting individual higher-risk operations and business relationships for in-depth mapping and risk assessment.

The scoping exercise does not necessitate complete or detailed mapping of an enterprise's entire value chain and related business relationships. Rather it expects companies to understand the general areas of risks and impacts they may be exposed to based on their sectors, specific sourcing models, or key business relationships. Many companies will be familiar with the most common risks prevalent within their sector and the geographies where their business partners are based or where they may be sourcing from; others may operate across sectors, products and geographies and find it challenging to prioritise between different RBC risk issues. Meaningful engagement with stakeholders and experts as part of the scoping exercise can help companies to make these assessments. In some cases, companies may discover, through their scoping and engagement with experts, that severe risks are most likely to arise in the downstream rather than upstream portion of the value chain; or that the risks they should prioritise under international standards are different to those they have traditionally focused on. For example, a retailer in the garment sector that prioritises specific labour rights may discover through its stakeholder engagement and scoping that other labour impacts are likely to be far more severe and urgent given their specific sourcing locations.

These early, high level scoping decisions are therefore important as they help to inform and shape how companies select individual suppliers for deeper-dive risk assessments and, on that basis, identify and address site-level impacts. The scoping exercise also helps to move companies away from traditional compliance-oriented approaches based on static codes of conduct and one-size-fits all approaches to supplier mapping, towards more proactive assessments of their own risk levels and where their greatest risks lie.

The importance of stakeholder and expert engagement in prioritisation decisions

Meaningful, two-way and good faith engagement[10] with relevant stakeholders and experts on prioritisation decisions and processes is critical as it helps to validate the company's own determinations of severity and likelihood at different points in the due diligence process. However, different stakeholders will be relevant to different prioritisation decisions, and OECD RBC standards take a flexible approach without prescribing which stakeholders companies should engage at specific points and in specific contexts.

Nevertheless, the OECD Due Diligence Guidance for RBC does include important specificity at particular points in the process. For example, it highlights the importance of engaging with experts in the context of the high level scoping exercise and prioritisation of RBC risk issues under Step 2.1 of the due diligence framework. It is important to engage subject matter and sector experts—such as relevant international civil society organisations, unions, academics and international organisations—as this stage in the process can often involve challenging decisions about where to focus resources and time; before moving on to map and then assess higher-risk business partners. In the context of site-level assessments and decisions about how to prioritise between and respond to identified impacts on the ground, the Due Diligence Guidance for RBC emphasises the importance of engagement with impacted and potentially impacted stakeholders and rightsholders and their representatives.

OECD RBC due diligence standards incorporate these and other principles and expectations for wider stakeholder engagement throughout the due diligence process. They also set out criteria for meaningful stakeholder engagement and guidance on engaging with specific vulnerable stakeholder groups.[11]

Ensuring that new and evolving risks feed into prioritisation processes

In addition to risk assessments of prioritised operations and suppliers under Step 2.2, companies are expected to regularly reassess their exposure to risks and impacts—such as prior to major decisions or changes in activity (e.g. market entry, product launch, policy change, or wider changes to the business); in response to or in anticipation of changes in the operating environment (e.g. rising social tensions); and periodically throughout the life of an activity or relationship.[12] Such reassessment can result in changes to prioritisation decisions where new, more significant issues are identified. Enterprises are also expected to monitor, track and review the effectiveness of their due diligence activities under Step 4 of the process. Where objectives and targets are not being met, they are called on to consider whether modifications to the due diligence process, including decisions made with respect to prioritisation, are necessary. This helps to ensure that companies' due diligence is effective, dynamic and adapted to their most severe risks at the time.

1.4. Ensuring that companies respond appropriately to identified risks and adverse impacts

International RBC due diligence standards also allow for flexibility in relation to the measures companies are expected to take in response to identified risks and impacts.

Proportionate and risk-based prevention and mitigation measures

The risk-based approach provides companies with flexibility by asking them to adapt and tailor their due diligence according to a range of factors—their size, sector and position in the value chain as well as the nature and level of risk they face in practice.

Proportionate, risk-based approaches are particularly important for smaller midstream and upstream actors to ensure that due diligence expectations are practicable. Tailoring due diligence to specific risks and impacts also guards against one-size-fits-all approaches and helps to ensure the measures a company takes are effective in identifying, mitigating, preventing or remedying the specific risk in the relevant local context. For example, traditional supplier audits based on on-site worker and supplier interviews may be an appropriate tool to identify safety issues at a manufacturing site, but tend to be far less effective in identifying other types of risks (e.g. child labour, intimidation, discrimination or anti-union behaviour), where more investigative approaches and different methods of stakeholder and worker engagement can be important.[13]

Practical and legal limitations and the role of leverage

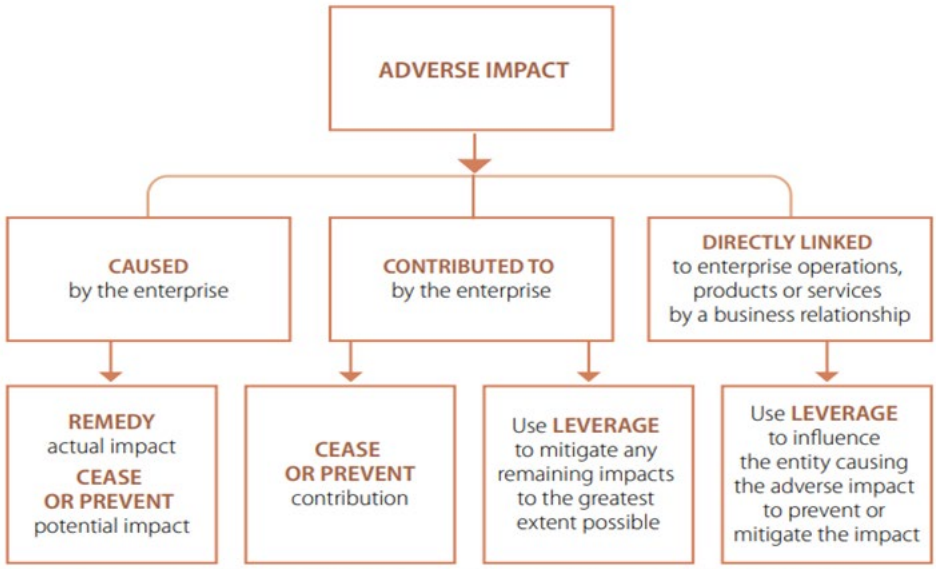
OECD RBC due diligence standards, like the UN Guiding Principles, also balance flexibility with more specific expectations through the "involvement framework". This differentiates between the due diligence expectations for companies depending on how they are involved with a specific risk or impact. For example, where companies **cause or contribute** to harm, they have a clear responsibility to stop the activities causing or contributing to harm (Step 3) and provide for or contribute to remedy, to the extent of their contribution (Step 6).[14] They should also take appropriate steps to prevent and mitigate future or remaining adverse impacts through a range of different measures (Step 3).

However, companies have more latitude in 'directly linked' scenarios—i.e. where a company is connected to an adverse impact through a direct or indirect business relationship. In these situations, international RBC due diligence standards expect companies to *seek to* prevent or mitigate adverse impacts by using a range of potential measures for supporting, collaborating with, and using and building leverage over, relevant business relationships. They recognise that the way a company seeks to

support or influence an individual business partner will depend on a range of legal and practical limitations. These include the degree of influence or leverage the company has over the business relationship in question, as well as laws of corporate governance (e.g. between shareholders and investee companies, boards and management, and parent companies and subsidiaries or joint ventures).[15]

This flexibility reflects the reality that different methods of engagement may be more effective in different contexts and for particular business partners—ranging from the use of business incentives (e.g. commitments to long-term contracts and future orders), to pre-qualification requirements, voting trusts, engagement with common buyers or joint investors, or participation in collaborative initiatives. Some companies will have regular dialogue with their suppliers and use that to work through issues; others may more effectively collaborate with joint buyers or investors to encourage effective action. Another method is to support suppliers through, for example, joint trainings or support for facility upgrading, or addressing systemic issues through collaborative approaches or engagement with governments. In this respect it is recognised, for example, that smaller enterprises in particular may not have the market power to influence their business relationships by themselves and thus might favour collaborative approaches.[16]

Figure 1. Addressing adverse impacts



Note: More specific guidelines for addressing human rights adverse impacts are listed in OECD (2011), Chapter IV.

Source: OECD Due Diligence Guidance for RBC (2018)

1.5. Demonstrating credible prioritisation processes and progress against outcome-oriented targets

As indicated above, giving companies too much discretion or allowing them to rely on the iterative, progressive nature of the risk-based approach risks leaving harms unaddressed—and victims without remedy. OECD RBC standards therefore expect companies to *demonstrate* credible prioritisation processes and meaningful progress against outcome-based targets through their public reporting (Step 5).

Reporting on how and why a company has prioritised its due diligence—including information on its most significant identified risks, prioritisation processes and criteria, and approaches to stakeholder engagement—help to build trust in its decision making and prioritisation processes. More transparency

about how a company has prioritised can also promote greater accountability where companies' prioritisation decisions are inconsistent with the risk-based principles and standards set out above. Similarly, the expectation that companies set and publish specific, time-bound and outcome-based targets and indicators for defining and measuring improvement on prioritised impacts is a critical part of demonstrating that decisions and actions are credible—and effective.

How an enterprise tracks its activities and outcomes on prioritised impacts, and how often, will vary according to the circumstances and the nature and severity of the relevant risk or impact and so the OECD Due Diligence Guidance for RBC incorporates a flexible, risk-based approach to the monitoring and tracking. In many cases, enterprises will need to look across a wide range of inputs (e.g. assessment data, data from grievance mechanisms or site level visits, desk-top reviews and worker or other stakeholder feedback). For example, if an enterprise seeks to track how well it is addressing child labour linked to specific direct or indirect suppliers, it will likely consider tracking progress both at the site-level (e.g. tracking progress of individual suppliers against correct action plans and tracking incidents of child labour identified and how they were handled) and at the global level (e.g. reviewing assessment data, reported grievances and credible reports across relevant high-risk suppliers or geographies). For severe impacts, there is a greater urgency to determine that adverse impacts are being effectively addressed. Explaining and justifying these activities publicly can help governments, investors, civil society and other stakeholders better understand and, as appropriate, challenge companies' decisions and track their progress over time.

2. Translating a risk-based due diligence approach into law

Where governments pursue mandatory due diligence legislation, it is important to preserve alignment with the core risk-based principles and expectations set out in internationally agreed RBC due diligence standards. The aims of the risk-based approach are highly relevant from a regulatory perspective—promoting proportionality for companies, tailored approaches and more effective and impactful outcomes for affected stakeholders.

How policymakers choose to translate the risk-based approach into law will have significant repercussions, shaping where companies focus their efforts—and how. It can also directly impact whether companies stay engaged and support business partners leading to positive development outcomes, or whether business choose to disengage from potentially high-risk contexts and business relationships, leading to outcomes that may run counter to the aims of legislation.

Implementing and assessing the quality of risk-based obligations and supply chain risk management is not a new concept for companies or governments, and existing regulatory expectations can be a useful model for policymakers, despite differences in scope and focus. A proportionate, risk-based approach is integral to, among others: anti-money laundering and terrorist financing; bribery and corruption; data protection; health and safety; product rules; food safety; and anti-slavery legislation. It is also integrated to varying degrees in existing human rights and environmental due diligence legislation.[17] Although approaches vary, these laws share the general principle of using a risk-based approach to focus business due diligence efforts on the risks that are most relevant and significant from a public policy perspective.

This section considers how policy makers can design RBC due diligence requirements that are effective and practicable in relation to the risk-based due diligence process. Drawing from examples of existing risk-based legislation, it presents options and considerations that can help to ensure that companies:

a) Prioritise appropriately on the basis of severity and likelihood
b) Put in place credible prioritisation processes
c) Respond appropriately to identified risks and adverse impacts
d) Demonstrate credible prioritisation processes and progress against outcome-based targets
e) Are not unreasonably sanctioned for adverse impacts that materialise in relation to risks they deprioritised

Box 4. The risks of one-size-fits all and zero tolerance approaches

Experience of risk-based approaches in the context of corruption, anti-money laundering and counter-terrorist financing, among others, highlights some of the potential dangers of zero tolerance and one-size fits all approaches. For example:

- The U.S. Department for Justice and the Securities and Exchange Commission have stated in relation to the U.S. Foreign Corrupt Practices Act (1977) that: "*One-size-fits-all compliance programs are generally ill-conceived and ineffective because resources inevitably are spread too thin, with too much focus on low-risk markets and transactions to the detriment of high-risk areas. Devoting a disproportionate amount of time policing modest entertainment and gift-giving instead of focusing on large government bids, questionable payments to third-party consultants, or excessive discounts to resellers and distributors may indicate that a company's compliance program is ineffective*."
- The Financial Action Task Force (FATF) has published extensive guidance papers on the risk-based approach (RBA) for public authorities and private sector actors in the context of its international standards on anti-money laundering and terrorist financing. FATF has made clear that "*the RBA is not a "zero failure" approach*" and that it allows countries and entities "*to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are reasonable and proportionate to the nature of risks*".

Sources: U.S. Department of Justice and U.S. Securities and Exchange Commission, 'A Resource Guide to the U.S. Foreign Corrupt Practices Act', second edition: https://www.justice.gov/criminal-fraud/file/1292051/download. Financial Action Task Force, 'Guidance for a Risk-Based Approach for Legal Professionals, 2019: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-legal-professionals.html and https://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate)

2.1. Ensuring appropriate prioritisation: severity and likelihood

Governments can take general or specific approaches to integrating risk-based principles into due diligence law and accompanying guidance. The level of detail that is appropriate will depend on different factors, including the scope of the law (e.g. sector-specific or issue-specific legislation tends to allow for more specificity in primary legislation), objectives in terms of changing company behaviour (e.g. due diligence, corporate reporting), and promoting legal certainty and proportionality.

Existing risk-based legislation is often issue or sector specific and so can afford to be more prescriptive on specific risks than a horizontal law with broad scope. However, even within a more restrictive scope of risk, the idea of prioritisation based on significance to the policy aims at hand is the same.

Laws take different approaches to defining risk significance. Some reference the degree of risk in violating the relevant law (e.g. U.S. Foreign Corrupt Practices Act, 1977) or a higher risk of, for example, money laundering occurring (e.g. the EU's 4th Anti-Money Laundering Directive 2015/849 on preventing the use of the financial system for money laundering or terrorist financing ('4th Anti-Money Laundering Directive'). The EU's 4th Anti-Money Laundering Directive adds specificity by prescribing specific high risk situations that require enhanced due diligence (e.g. cross-border correspondent relationships with a third-country respondent institution or transactions or business relationships with politically exposed persons).[18]

In other cases, policymakers have defined specific significant risks—or a list of minimum significant risks—that they require companies to address. For example, the EU Conflict Minerals Regulation 2017/821 requires companies to base their due diligence on a supply chain policy that "*that*

conforms to Annex II to the OECD Due Diligence Guidance outlining the risks of significant adverse impacts which may be associated with the extraction, trade, and handling of minerals in and export of minerals from conflict-affected and high-risk areas".[19]

The EU General Data Protection Regulation 2016/679 presents 'high risk' as: "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is* ***likely to result in a high risk to the rights and freedoms of natural persons****".* Accompanying Guidelines help determine whether processing is "likely to result in a high risk",[20] and the law itself also specifies non-exhaustive examples of high risk:

> *"(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
>
> *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
>
> *(c) a systematic monitoring of a publicly accessible area on a large scale."*[21]

Examples of existing anti-slavery and human rights and environmental due diligence legislation explicitly list severity and probability (likelihood) as criteria to inform due diligence, either in the text of the law or in statutory guidance. However, they do not always define severity.

For example, Norway's Transparency Act (2021) states that "Due diligence shall be carried out regularly and in proportion to the size of the enterprise, the nature of the enterprise, the context of its operations, and the *severity and probability* of adverse impacts on fundamental human rights and decent working conditions"; whereas these terms are not further defined in the law.[22]

The French *Loi de Vigilance* (2017) applies to severe risks as well as potential and actual impacts, but does not define severity[23]. Similarly, the EU General Data Protection Regulation 2016/679 sets out the basic responsibility of data controllers to take appropriate measures, with reference to likelihood and severity, but does not define the terms:

> *"taking into account the nature, scope, context and purposes of processing as well as the risks of varying* ***likelihood and severity for the rights and freedoms of natural persons****, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary".*[24]

The Australian Modern Slavery Act (2018) goes further, by clarifying that companies may need to prioritise risks on the basis of severity, and **defining severity on the basis of the UN Guiding Principles on Business and Human Rights** (Principle 24): *"This means those risks that have the greatest scope (gravest impact) or scale (number of people affected) or where delayed response would make them irremediable (for example, because delay would cause loss of life or loss of education)."*[25]

Some due diligence and anti-slavery laws depart from the significance framework in these examples and under international standards (see Section 1.2 of this note). For example, some laws lack clarity on the role and limitations of leverage and influence over business partners in the due diligence process. Others include the ability to influence over a business partner as a factor in determining whether a due diligence process or activity is "appropriate", without making clear that leverage should not be a driving factor in how companies prioritise their due diligence in accordance with international standards.

Other examples diverge from the significance framework set out in international standards in other ways, depending on policy objectives. Examples include requiring covered entities to focus their due

diligence on longer-term or "established" business partners, or in prescribing a negligible level of overall risk for all covered entities.

Considerations for policy makers

Where policymakers pursue mandatory human rights and environmental due diligence legislation, it is important that they align definitions of significance with internationally agreed RBC due diligence standards in order to ensure that companies prioritise consistently and effectively across jurisdictions, without giving undue weight to other factors. This means defining significance on the basis of severity and likelihood (or probability) of adverse impacts, with severity defined according to the three factors of scope, scale and irremediability (see Section 1). Governments can also integrate further specificity and guidance on risk severity, including indicators of severity for specific risks. They can also introduce specific criteria to ensure that prioritisation processes are credible (see below).

Other factors—such as proximity to or influence over a business partner, the long-term nature of a relationship, or the company's connection to the harm (i.e. whether it caused, contributed to or is directly linked to it)—are very relevant to how companies are expected to *respond* to prioritised impacts. But they are not relevant to the prioritisation decision process, as explained in Section 1. Allowing companies to depart from the significance framework set out in international standards and that governments have already endorsed can have important drawbacks. It can lead to companies spending time and resources on mapping and evaluating entities in the value chain that are likely to be low-risk and tends to be counter-productive to the aims of RBC due diligence (see Section 1).

2.2. Ensuring credible prioritisation processes

This section discusses how far existing risk-based legislation integrates specific expectations to ensure that companies' prioritisation processes are credible and consistent with international standards. It sets out considerations for policymakers on these elements, which can help to promote greater legal certainty for companies as well as greater trust in companies' prioritisation decisions:

- The role of "risk factors" in prioritisation decisions
- The importance of stakeholder and expert engagement
- Ensuring that new and evolving risks feed into prioritisation processes

The role of potential "risk factors" in prioritisation decisions

The expectation under the OECD Due Diligence Guidance for RBC that companies consider contextual risks on the basis of **sector, geographic, product and enterprise-level "risk factors"** under Step 2.1 (see Box 2)*, prior to* identifying and prioritising specific business partners for mapping and in-depth assessment, is reflected in other risk-based approaches and laws. Although these examples tend to be risk-specific, and so set narrower expectations, the broad principle still applies.

Risk factors—indicators or variables of potentially high or low risk—can give companies greater legal certainty about how to prioritise, by helping to guide them towards the risks that are most relevant to them in light of the specific sector and geographies they operate in, invest in or source from, the types of business partners they engage with, and the nature of their products, transactions or services. They can be mandatory, or illustrative and non-exhaustive. They can be set out in the text of the primary law or in secondary legislation or accompanying interpretative guidance (or all of these). They can also vary in granularity, depending on, for example, the scope of the law and the degree of legal certainty that governments seek to provide for companies.

For example, the **UK Modern Slavery Act (2015)** sets out the UK government's legal requirements for how organisations must address and report on modern slavery, including a requirement on commercial organisations with an annual turnover of more than £36 million to report annually on the steps, if any, they have taken to ensure modern slavery is not taking place in their organisation and supply chains. The UK Act is light on detail and does not mandate what should be reported in the annual statement or how companies should carry out risk-based due diligence. However statutory guidance lists **"business risks"—including country risks, sector risks, transaction risks and business partnership risks—** that companies are expected to consider in assessing and managing risks to workers (see Box 5).

Box 5. Risk factors: UK Modern Slavery Act

Statutory guidance for businesses on transparency in supply chains under the UK Modern Slavery Act (2015) lists the following risk factors:

- **"Country risks** – exposure may be greater in global supply chains in countries where protection against breaches of human rights are limited, particularly with regard to rights of foreign contract workers to retain their own ID and papers, and/or where work arrangement by agents is common, etc.
- **Sector risks** – there are different risks and levels of risk in different sectors. For example, the risks and arrangements which generate bonded labour situations for workers in the extractives sector may differ to those causes in manufacturing.
- **Transaction risks** – banks or financial institutions may be involved in facilitating financing from or supporting cases of modern slavery and bonded labour in operations or supply chains or through money laundering.
- **Business partnership risks** – Different supplier relationships and business partnerships will all carry different levels of risks. In some cases, existing long-term partnerships will involve less risk because the organisation will have a better knowledge of their partner's operations and policies. However, a new partnership or business relationship may be equally low risk as long as proper due diligence is conducted."

Source: U.K. Home Office, Statutory guidance for business on Transparency in Supply Chains (2021), https://www.gov.uk/government/publications/transparency-in-supply-chains-a-practical-guide

Accompanying Guidance to the German Act on Corporate Due Diligence Obligations in Supply Chains ('German Supply Chain Act') (2021) clarifies that the German government expects companies to carry out high level, "abstract" risk scoping on the basis of **sector-specific and country-specific risk factors**, before carrying out more specific or "concrete" and iterative entity-level risk assessments.[26]

Guidance by the U.S. Department of Justice and Securities and Exchange Commission on the **U.S. Foreign Corrupt Practices Act (1977)** similarly expects companies to take into account a broad, indicative list of risk factors, such as: *"risks presented by: the country and industry sector, the business opportunity, potential business partners, level of involvement with governments, amount of government regulation and oversight, and exposure to customs and immigration in conducting business affairs".* [27]

The **EU General Data Protection Regulation (EU) 2016/679**[28], which requires data protection impact assessments in situations that are *"likely to result in a high risk to the rights and freedoms of natural persons",* requires the **supervisory authority to "establish and make public a list of the kind of processing operations** which are subject to the requirement for a data protection impact assessment" and the option to establish and publish a list "of the kind of processing operations for which no data protection impact assessments is required".

Existing standards and legislation on anti-money laundering and counter-terrorism financing provide helpful models, even if they may be too granular for cross-sectoral RBC due diligence legislation with broad scope. For example, a risk-based approach is central to the Financial Action Taskforce Recommendations (2012) ('FATF Recommendations')[29], international standards on combating money laundering and the financing of terrorism which have been endorsed by over 180 countries. The Recommendations set standards for requiring financial institutions and designated non-financial businesses and professions ('DNFBPs') to identify, assess and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks. They include specific recommendations for financial institutions and DNFBPs to undertake customer due diligence using a risk-based approach:[30]

> *"The general principle of a [risk-based approach] is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing."*[31]

The FATF Recommendations introduce the concept of **"risk variables**" that financial institutions and DNFBPs should consider when assessing risks relating to specific types of customers, geographies and particular products, services, transactions and delivery channels—such as the purpose of an account or relationship and the size of transactions undertaken.[32] They recommend that **enhanced due diligence** is applied in specific, mandatory situations[33], and when higher risk scenarios are otherwise identified. Interpretative Notes set out indicative, non-exhaustive examples of "**potentially higher risk situations" under three categories of risk factors**: customer risk factors, country or geographic risk factors and product, service, transaction or delivery channel risk factors (see Box 6).

They also propose that **simplified due diligence** may be reasonable in low-risk contexts, provided that there has been "adequate analysis of the risk", a lower risk has been identified, all relevant risk factors have been have been considered and other requirements are fulfilled. Interpretative Notes provide examples of **"potentially lower risk situations"** using the same three categories of risk factors (see Box 6).[34]

The Recommendations qualify the use of low-risk factors further. For example, they make clear that simplified customer due diligence measures "*are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply*".[35] In addition: "*Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of [customer due diligence] measures, in particular for ongoing monitoring of transactions*".[36] See 'Recommendations' below.

Box 6. Risk factors: International standards on anti-money laundering and countering terrorist financing (AML/CFT)

The Financial Action Taskforce (FATF) Recommendations recommend that financial institutions and DNFBPs carry out due diligence using a risk-based approach, and consider "all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied". Interpretative Notes on the risk-based approach set out indicative, non-exhaustive examples of potentially higher-risk situations and potentially lower-risk situations in the form of "risk factors.

Examples of potentially higher-risk situations include, for example:

(a) "**customer risk factors**":

- the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer);
- businesses that are cash-intensive;
- the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(b) "**country or geographic risk factors**":

- countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate anti-money laundering or counter-terrorist financing (AML/CFT) systems;
- countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country

(c) "**product, service, transaction or delivery channel risk factors":** private banking; anonymous transactions; non-face-to-face business relationships.

Examples of situations **of potentially lower-risk situations** include, for example:

- **Customer risk factors**: public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- **Country risk factors:** countries identified by credible sources as having effective anti-money laundering and counter-terrorism financing systems, or a low level of corruption or other criminal activity.

FATF has also published extensive guidances and best practices on implementation of the FATF Recommendations, including implementation of the risk-based approach, key risk-based principles and sector-specific indicators, risk factors and red flags.

Note: Risk factors are presented as illustrative guidance only and "are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances".
Source: FATF Recommendations (2012) – amended March 2022. See in particular Recommendations 1 and 10, including Interpretative Notes

The EU's 4th Anti-Money Laundering Directive[37]— one of the pillars of the EU's legislation to combat money laundering and terrorist financing—broadly follows the FATF approach and requires covered entities to apply "risk-sensitive" customer due diligence in specific circumstances—with simplified and enhanced due diligence in situations of low or high risk.[38] The Directive requires Member States to ensure that covered entities take into account, at a minimum, a non-exhaustive list of general "**risk variables**" in determining risk levels[39]: "*(i) the purpose of an account or relationship; (ii) the level of assets to be deposited by a customer or the size of transactions undertaken; (iii) the regularity or duration of the business relationship."*

In assessing risk, entities are also expected to take into account **minimum indicative risk factors** of potentially low and high risk set out in Annexes to the law. These include **customer risk factors; product, service, transaction or delivery channel risk factors; and geographical risk factors**. Like the FATF Recommendations, the 4th Anti-Money Laundering Directive sets out specific situations that require **mandatory enhanced due diligence**, such as "*when dealing with natural persons or legal entities established in the third countries identified by the Commission as high-risk third countries, as well as in other cases of higher risk that are identified by Member States or obliged entities"* (Article 18(1)).

Accompanying "**Risk Factors Guidelines**"[40] prepared by the European Supervisory Authorities include additional guidance on risk factors, which they define as "variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship or occasional transaction". The European Banking Authority has since published revised **Guidelines on Risk Factors** which set out sector-specific guidance and seek to promote a common understanding, by firms and competent authorities, of what the risk-based approach to AML/CFT entails and how it should be applied. It clarifies the expectation that entities should take a "holistic view" of their risks as a general principle—independent from their individual, entity-level risk assessments.

Considerations for policymakers

To assist companies with their prioritisation of RBC risk issues and promote greater legal certainty about what a credible prioritisation process looks like, policymakers can consider:

- **Requiring companies to carry out an initial, high-level and holistic "scoping exercise**" in order to identify their most significant risk areas and, on that basis, their highest-risk operations and business relationships, consistent with Step 2.1 of the OECD Due Diligence Guidance for RBC, and building on approaches to anti-money laundering and terrorist financing due diligence;
- **As part of their scoping exercise, requiring companies to take into account mandatory or indicative, non-exhaustive risk factors**. Governments can also consider developing more specific sector or issue specific risk factors in secondary legislation or accompanying guidance. **See Annex A of this document for illustrative examples of risk factors of potentially higher risk;**
- **Rebuttable presumptions of high risk situations**, based on the approach taken in the context of the EU General Data Protection Regulation.[41]
- **Providing other indicative sources of information or indicators of risks and red flags**. Lists of information based on external sources should be regularly monitored and updated in order to be credible.

In all of these cases, it is important to ensure that risk-based due diligence legislation reflects the context-specific nature of human rights and environmental risks and avoids predetermining entire countries or products or services as either high-risk or low-risk.

The role of stakeholder and expert engagement in prioritisation

Existing risk-based laws adopt different approaches to stakeholder and expert engagement, depending on the specific risk issue (e.g. stakeholder engagement requirements are more common in relation to human rights laws), and the focus of the law (e.g. corporate disclosure or due diligence). Existing anti-slavery, human rights and environmental due diligence legislation tend to adopt general rather than specific approaches to stakeholder and expert engagement. They are generally not explicit about the role of stakeholder and expert engagement in informing and validating prioritisation decisions and determinations about the relative severity and probability of individual risks or impacts.

The UK Governments' statutory guidance on the **UK Modern Slavery Act (2015)**, for example, states only that human rights due diligence "requires consultation with stakeholders that are potentially or actually affected…. particularly vulnerable groups". The role of stakeholder engagement in connection with prioritisation decisions—whether in the context of risk scoping, selecting individual business partners for in-depth risk assessments, or in prioritising impacts for action—is not explicitly addressed.[42]

The **French *Loi de Vigilance* (2017)** requires enterprises to draw up vigilance plans "in conjunction with stakeholders of the company", including as part of "multi-stakeholder initiatives within sectors or at territorial level", and the complaint mechanism is developed with workers' representatives. The **German**

Supply Chain Act (2021) requires companies, in establishing and implementing their risk management system, to "*give due consideration to the interests of its employees, employees within its supply chains and those who may otherwise be directly affected in a protected legal position by the economic activities of the enterprise or by the economic activities of an enterprise in its supply chains*". However, the law does not specifically address stakeholder or expert engagement in the context of prioritisation. [43]

Considerations for policymakers

Policymakers can consider requiring companies to carry out meaningful and risk-based engagement with stakeholders and experts as a necessary element of a credible prioritisation process (see Section 1.2 of this document). However, it is important that legislation avoids overly prescriptive requirements about which stakeholders are relevant to a company in a specific context and sector (see Section 1.3 of this document).

Given the degree of flexibility this approach gives to individual companies, governments can consider promoting greater legal certainty in ways that are consistent with international standards. For example, by:

- **Clarifying the prioritisation activities and decisions that will likely require stakeholder engagement,** such as a) the prioritisation of high level RBC risks issues during the companies' risk scoping exercise, b) the selection of higher-risk operations and business partners on the basis of the risk issues prioritised c) prioritising between specific identified site-level impacts that require action under Step 3 of the six-step due diligence framework.
- **Clarifying the broad groups of stakeholders and experts that are likely to be relevant to key prioritisation processes and decisions**. For example, experts will be most relevant during the initial risk scoping exercise, when companies are expected to consider the relative severity and likelihood of the human rights and environmental risks they face. However, when identifying and prioritising between site-level impacts, engagement with impacted or potentially impacted stakeholders or their representatives is critical.
- **Requiring companies to disclose how they have engaged stakeholders and experts in their prioritisation activities and decisions** (see below).

Ensuring that new and evolving risks feed into ongoing prioritisation

Existing risk-based laws and standards reflect the ongoing, iterative nature of due diligence, and require companies to carry out regular risk assessments and ongoing monitoring. They also expect companies to move on to address de-prioritised risks and impacts once they have addressed their most severe risks.

For example, the FATF Recommendations (2012) expect financial institutions to conduct "ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship"[44]. The EU's 4th Anti-Money Laundering Directive specifies that customer due diligence measures include "ongoing monitoring of the business relationship…throughout the course of that relationship" with "enhanced, ongoing monitoring" in higher risk circumstances (e.g. with respect to transactions or business relationships with politically exposed persons).[45]

Statutory guidance to Australia's Commonwealth Modern Slavery Act (2018) emphasises the importance of ongoing prioritisation: "*Prioritising which risks you respond to first does not mean you can disregard the risks that you de-prioritise. Once you have addressed your most severe risks, you should ensure you move on to address these other risks*." [46]

Considerations for policymakers

To ensure that companies carry out **proactive and ongoing risk-based prioritisation** consistent with international standards, policymakers can consider requiring companies to:

- Integrate new and emerging risks into their risk management and prioritisation processes; and
- Move on to address other identified risks and impacts, once they have addressed prioritised actual and potential impacts.

Ensuring that companies have effective processes in place to **identify and prioritise** risks and impacts as they evolve and emerge is of course also key—for example, through requirements for comprehensive risk assessments that incorporate meaningful stakeholder engagement (Step 2.2); ongoing monitoring and periodic assessments to track progress on prioritised impacts, including through meaningful engagement with impacted or potentially impacted stakeholders or their representatives and experts (Step 4) and effective complaints mechanisms (Step 6).

2.3. Ensuring that companies respond appropriately to identified risks and adverse impacts

Proportionate and risk-based measures

Even if definitions of risk differ, examples of legislation broadly reflect the principle that responses to identified risks or impacts should be proportionate and risk-based (i.e. tailored to the nature and significance of the risk) (see Section 1.4 of this note). Laws variously require companies to put in place "appropriate", "reasonable" or "effective" prevention and mitigation measures in a particular context, tailored to the level of risk that they face.

The **EU's 4th Anti-Money Laundering Directive**, for example, requires Member States to "*ensure that obliged entities have in place policies, controls and procedures to **mitigate and manage effectively** the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity. Those policies, controls and procedures shall be **proportionate** to the nature and size of the obliged entities*". The Directive combines due diligence requirements in specific, predefined high risk situations with broader risk-based principles. For example, it requires Member States to ensure that obliged entities may determine the extent of their customer due diligence measures "on a risk-sensitive basis"[47]. Entities are expected to apply enhanced customer due diligence measures to higher risk situations and to manage and mitigate those risks "appropriately". European Supervisory Authorities, who were tasked to develop separate guidelines on appropriate measures, have defined the risk-based approach as "*an approach whereby competent authorities and firms identify, assess and understand the ML/TF risks to which firms are exposed and take AML/CFT measures that are proportionate to those risks*".[48]

In the context of laws relating to data protection and human rights and environmental due diligence:

- The **EU's General Data Protection Regulation (2016/679)** requires data controllers to take into account factors including the likelihood and severity for the rights and freedoms of natural persons. The regulation specifically requires that data controllers "implement appropriate technical and organisational measures" to ensure and demonstrate compliance, by taking into account the "nature, scope, context and purposes of processing" and the "risks of varying likelihood and severity for the rights and freedoms of individuals".[49]
- France's ***Loi de Vigilance* (2017)** requires companies' vigilance plans to include "reasonable vigilance measures" and "appropriate action to mitigate risks or prevent serious violations", however the law does not provide further specificity.
- Norway's ***Transparency Act* (2021)** requires that due diligence is carried out "regularly and in proportion to the size of the enterprise, the nature of the enterprise, the context of its operations, and the severity and probability of adverse impacts on fundamental human rights and decent working conditions".

However, some legislation departs from risk-based principles by introducing much more prescriptive requirements for the mitigation and/or prevention measures companies should put in place. The **German Supply Chain Act (2021)** includes elements of the risk-based approach with prescriptive requirements for the preventive measures companies should put in place—differentiated between own operations ("area of business") and vis-à-vis direct suppliers. For example, it requires "appropriate and effective risk management" and "appropriate measures"' that take into account a range of factors, including the severity and probability of the risk. However, it also mandates specific preventive measures that should be applied in relation to direct suppliers, such as contractual assurances and related trainings and control mechanisms.[50]

Practical and legal limitations and the role of leverage

As discussed in Section 1.4 of this note, international RBC due diligence standards use the "involvement framework" to differentiate between how a company is expected to respond to an actual or potential impact, depending on whether it is causing or contributing to the harm or directly linked to it through a business relationship.[51]

Existing legislation varies in the degree to which it integrates the involvement framework and, linked to this, whether it recognises the practical and legal limitations to how a company should respond in directly-linked situations. While existing laws recognise that the degree of leverage or control a company has over a specific business partner will influence what an appropriate response looks like in a particular context, they are not always clear about the circumstances in which leverage is a relevant factor that companies can take into account—and when it is not.

Considerations for policymakers

It is important to ensure that, where companies cause or substantially contribute to harms, they are responsible for ceasing the activities causing or contributing to harm, and providing for remediation consistent with international due diligence standards. However, different expectations should apply where a company is directly linked to a harm through a business relationship. In these situations, a company should be responsible for demonstrating that it is making sufficient efforts to support, use and build influence over business partners in order to prevent or mitigate the harm; the company should not be held directly responsible for ceasing or remediating harm. Governments may consider, for example, consistent with international due diligence standards:

- **Allowing for differentiated, risk-based and proportionate prevention and mitigation** responses to prioritised adverse impacts on the basis of i) the involvement framework (ie. whether the company has caused, contributed to or is directly linked to the impact; and ii) legal and practical constraints, including the extent of leverage and influence over business relationships;
- **Requiring enterprise to carry out good faith, proportionate and risk-based efforts to use their leverage and, where enterprises lack leverage, seek to increase their leverage** vis-a-vis relevant business relationships, with optional measures or illustrative examples;
- **More specific requirements for particular scenarios**, for example to ensure that disengagement is a measure of last resort and, where undertaken, is done responsibly and on the basis of appropriate triggers;
- **Requiring entities to demonstrate publicly and/or on the reasonable request of the supervisory authority that their responses are appropriate in the circumstances**: proportionate, risk-based, and based on continual improvement (see below).

2.4. Demonstrating credible prioritisation processes and progress against outcome-oriented targets

Existing laws expect companies to demonstrate appropriate due diligence through public disclosure or by reporting to supervisory authorities, but in different ways and with different levels of prescription. They vary in the extent to which they explicitly require disclosure against targets and indicators to demonstrate continual progress, or information on companies' most significant risks and impacts, their prioritisation processes and stakeholder engagement.

For example, the **French *Loi de Vigilance* (2017)** requires companies to report on implementation of their vigilance plans and expects their plans to include "appropriate action to mitigate risks or prevent serious violations", with very limited specificity about the content of the plan. Other laws include more specificity. For example, statutory guidance to the **UK Modern Slavery Act (2015)** highlights the importance of public performance indicators in demonstrating progress over time and provides examples of targets and key performance indicators.[52]

Some laws require companies to disclose information on their most significant risks and impacts. For example, **Norway's Transparency Act (2021)** requires enterprises to publish:

- A general description of the enterprise's structure, area of operations, guidelines and procedures for handling actual and potential adverse impacts on fundamental human rights and decent working conditions;
- Information regarding **actual adverse impacts and significant risks of adverse impacts** that the enterprise has identified through its due diligence; and
- Information regarding measures the enterprise has implemented or plans to implement to cease actual adverse impacts or mitigate **significant** risks of adverse impacts, and the results or expected results of these measures.

The **German Supply Chain Act (2021)** requires an annual public report, with specific minimum content requirements—including:

- Whether the enterprise has identified risks or violations and, if so, which ones;
- What due diligence the enterprise has carried out and the measures taken;
- How the enterprise assesses the impact and effectiveness of the measures; and
- What conclusions it draws for future measures.

However, the law does not reference public time-bound outcome-based targets or explicitly require information on prioritisation processes, decisions or criteria, or engagement with relevant stakeholders and experts.

Other risk-based laws and standards prioritise reporting to supervisory authorities, sometimes accompanied by optional or recommended public disclosure. For example, the **FATF Recommendations (2012)** call for financial institutions and designated non-financial businesses and professions to document their risk assessments *"in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs*".[53]

The EU's General Data Protection Act 2016/679 requires entities to communicate data protection impact assessments to the supervisory authority in case of prior consultation or if requested by the Data Protection Authority. Guidelines under the Act state that publishing an impact assessment is not a legal requirement, however it recommends that "controllers should consider publishing at least parts, such as a summary or a conclusion of their [data protection impact assessment]". [54] They further explain that "*The purpose of such a process would be to help foster trust in the controller's processing operations, and*

demonstrate accountability and transparency. It is particularly good practice to publish a [data protection impact assessment] where members of the public are affected by the processing operation." The law is accompanied by extensive 'Guidelines on Transparency'.[55]

Considerations for policymakers

To ensure that companies are able to demonstrate credible risk-based prioritisation processes and decisions, as well as measurable progress against time-bound, outcome-based targets, governments can require enterprises to, consistent with the OECD Due Diligence Guidance for RBC:

- **Track activities and outcomes** in relation to prioritised impacts using **specific, time-bound** and **outcome-oriented targets and indicators**;
- **Disclose** their appropriate and time-bound **targets and indicators**, and information to demonstrate progress and outcomes against those indicators; and
- **Disclose prioritised RBC risk issues** and information on their **prioritisation criteria** and processes, including stakeholder engagement processes, prioritised impacts, outcomes and provision of and co-operation in remediation.

In order to evaluate the quality and credibility of company's prioritisation efforts, governments can also consider requiring companies to disclose additional, more granular information to the supervisory authority, on its reasonable request. This information could include, for example:

- Information on the company's **prioritised high risk operations and business relationships**, including the company's detailed risk mapping (with due consideration for business confidentiality concerns);
- The **stakeholders and/or experts** that the company consulted with in the context of its due diligence, or, where the company did not consult, a reasonable justification for not doing so;
- For **severe adverse impacts that are identified but not prioritised**, a reasonable justification for the prioritisation decision;
- Prevention and mitigation **action plan(s),** where available; and
- More specific information on the provision of and co-operation in **remediation.**

Governments can also consider public reporting templates and accompanying guidance on public reporting and on setting quantifiable targets and indicators based on best practice. For example, requiring reporting on environmental impacts against science-based mitigation targets.

2.5. Ensuring that companies are not unreasonably sanctioned for adverse impacts that materialise in relation to risks they deprioritised

It is important that governments do not unreasonably sanction companies where they have demonstrated credible prioritisation processes and otherwise taken appropriate and effective measures in accordance with the law. Companies will necessarily deprioritise and out-scope some RBC risk issues and adverse impacts during the prioritisation process; it is not realistic to expect companies to identify and address all possible potential RBC impacts linked to their operations and across the entirety of value chains simultaneously.

Exceptions may include, for example if the deprioritised impact becomes more severe or likely and the company was aware of the fact (e.g. through complaints mechanisms), or it was reasonably foreseeable that the company would be aware (e.g. as a result of public allegations in relation to a particular supplier). Companies could also be responsible for deprioritised impacts in directly linked scenarios if they did not prioritise in good faith or otherwise in accordance with the law (for example, where they prioritise impacts

on the basis of how easy they are to address or where they sit in the value chain—rather than on the basis of their severity) .

In determining whether or not a company should be sanctioned in relation to adverse impacts that it deprioritised (and so did not prevent, mitigate or remedy itself, or did not influence a business relationship to prevent, mitigate or remedy), it is important that supervisory authorities consider:

- **Whether or not the company is able to demonstrate credible, appropriate and good faith prioritisation**, taking into account the enterprise's public reporting on its prioritisation process, criteria and justifications and, if relevant, other evidence disclosed by the company to the supervisory authority
- **The foreseeability of the adverse impact, and whether or not it should reasonably have been prioritised for prevention, mitigation and/or remedy** by the enterprise, taking into account its circumstances—including its position in the supply chain, nature of its products and services and degree of influence or control over relevant business relationship
- **Whether any mitigation and prevention activities carried out by the enterprise in relation to the adverse impact were appropriate** (i.e. risk-based and proportionate), taking into account the enterprise's circumstances.

Box 7. Risk-based enforcement: the U.S. Foreign Corrupt Practices Act (FCPA)

Guidance by the U.S. Department of Justice and Securities and Exchange Commission under the U.S. FCPA states that:

"*DOJ and SEC will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program, even if that program does not prevent an infraction in a low risk area because greater attention and resources had been devoted to a higher risk area. Conversely, a company that fails to prevent an FCPA violation on an economically significant, high-risk transaction because it failed to perform a level of due diligence commensurate with the size and risk of the transaction is likely to receive reduced credit based on the quality and effectiveness of its compliance program.*"]

Source: U.S. Department of Justice and U.S. Securities and Exchange Commission, 'A Resource Guide to the U.S. Foreign Corrupt Practices Act', second edition: https://www.justice.gov/criminal-fraud/file/1292051/downloadSource:

3. Conclusion

The flexibility inherent to risk-based due diligence is key to achieving the public policy aims of RBC due diligence laws. It helps to ensure that companies commit their time and resources efficiently and effectively to where their risks are greatest and most urgent. However, giving companies too much discretion in how they find and manage risk can leave significant harms unaddressed—and victims without remedy. It is therefore important that policymakers combine risk-based expectations with specificity on key issues of concern in a way that is consistent with international due diligence principles and that does not create unintended consequences. The ultimate aim of responsible business conduct is for enterprises to contribute to addressing and improving problems rather than disengaging from them, and legislation should seek the right balance to achieve this.

Clear requirements to ensure that companies prioritise appropriately, meaningfully engage with relevant stakeholders and demonstrate credible processes and progress against outcome-based targets, for example, will all be key. But allowing companies some flexibility also means providing them with protections where they prioritise in good faith and in accordance with the law. Business should therefore not be unreasonably sanctioned for harms they deprioritise or which they could not have reasonably foreseen. In this respect when designing due diligence legislation policymakers should consider provisions which direct companies to:

- **Prioritise consistently and effectively on the basis of severity** and likelihood across jurisdictions, without giving undue weight to other factors (Section 2.1).
- **Put in place credible prioritisation processes** (Section 2.2), including through:
  - Carrying out an initial, high-level scoping exercise, taking into account “risk factors”, in order to identify their most significant risks areas and, on that basis, their highest-risk operations and business relationships;
  - Carrying out meaningful and risk-based engagement with relevant stakeholders and experts on prioritisation decisions;
  - Integrating new and emerging risks into ongoing prioritisation.
- **Respond appropriately to identified risks and impacts**, including, where a business partner has caused the harm, by recognising legal and practical constraints—such as they extent of leverage or influence over the business partner in question (Section 2.3).
- **Demonstrate credible prioritisation processes and progress against outcome-oriented targets** (Section 2.4).

Related and important questions merit further consideration by policymakers: how can prescriptive expectations be integrated into legislation to increase legal certainty without undermining core risk-based principles? How can policymakers incentivise responsible engagement, not de-risking? How can policymakers apply the same risk-based principles to their enforcement mechanisms, and learn from existing approaches to ensure that risk-based enforcement approaches are consistent and effective?

Annex A. Illustrative examples of risk factors for RBC due diligence legislation

This Annex sets out illustrative examples of risk factors for potentially high-risk situations, for consideration in the context of mandatory human rights and environmental due diligence. The list is indicative and is not intended to be comprehensive. It is based on the risk factors set out in OECD Due Diligence Guidance for RBC.

For example:

1) **Enterprise-level risk factors**: Enterprise-level risks are risks associated with a specific company, supplier or core business relationship, including public enterprises, such as weak governance, a poor history of conduct in relation to respecting human rights, labour rights, anti-corruption standards, environmental standards, or a lack of culture around responsible business conduct.

   For example:

   (a) Enterprises that do not have public policies or reports on relevant human rights and environmental issues or due diligence;

   (b) Enterprises subject to allegations of human rights or environmental abuses by independent experts, civil society organisations, trade unions, international organisations or the media within a specified time, or which have been subject to repeated allegations of human rights and/or environmental abuses;

   (c) Enterprises that rely on informal employment or precarious work, whose workers live on-site or where workers are paid in cash;

   (d) Entities that carry out particularly dangerous activities, such as mining in conflict zones or provision of private security services.

2) **Business-model risk factors:** Business-model risks are risks associated with an enterprise's business model that may impede the ability of business relationships to implement due diligence policies and expectations.

   For example:

   (a) Business-models with numerous and highly diversified product lines;

   (b) Business-models with short-term product cycles;

   (c) Business-models that involve a high proportion or late or delayed payment or a high proportion of late, cancelled or changed orders;

   (d) Franchising models that are associated with low labour protections;

3) **Sourcing-model risk factors:** Sourcing-model risks are risks associated with how enterprises source and the diversity and nature of their business relationships.

   For example:

(a) Sourcing-models that involve a very large number of suppliers in relation to the size of the enterprise and its due diligence resources

(b) Sourcing models that involve a high percentage of short term relationships with suppliers or other business relationships;

(c) Sourcing models that rely on indirect sourcing practices with limited selection processes for relevant intermediaries or visibility over relevant business relationships;

(d) Sourcing models that involve a high number of sourcing countries relevant to the enterprise's size and resources.

4) **Product, service or transaction risk factors:** Product, service or transaction risks are risks related to inputs or production processes used in the development or use of specific products, or specific types of services or transactions.

For example:

(a) Products associated with the generation of dangerous, hazardous or toxic substances, or whose end-use, misuse or over-use is inherently dangerous or harmful (e.g. military or dual use products);

(b) Products that contain significant volumes and/or value of raw materials commonly associated with higher environmental and/or human rights risks;

(c) Products whose production is commonly associated with adverse impacts such as deforestation or forced labour;

(d) Loan services or transactions, including sales or marketing contracts, that pose severe risks to human rights or the environment;

(e) Services associated with high risks of misuse or resale of data, or which can be used as a tool to incentivise or facilitate another entity to carry out human rights abuses.

5) **Geographical risk factors:** Geographic risks are conditions in a particular region, area or country which may make sector risks more likely. Geographic risk factors can generally be classified as those related to the regulatory framework, governance, socio-economic context and political context.

For example:

(a) Regions that are associated with severe adverse environmental impacts, including severe climate change impacts;

(b) Regions that are associated with heightened risks to vulnerable groups, such as high degrees of vulnerable and/or discriminated populations; continuing restrictions on the freedom of association of an entire workforce, or serious discrimination against all members of a minority group;[56]

(c) Regions subject to higher-risk political contexts such as ongoing armed conflict;

(d) Regions or countries identified by credible sources, such as mutual evaluations or credible third party reports, as not having effective governance (rule of law, level of corruption, strength of inspectorates) or regulatory frameworks (e.g. weak labour, human rights or environmental protection laws that do not align with international standards, including, where relevant, inadequate legal protection of indigenous peoples and other vulnerable populations);

(e) Countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;

(f) Regions or countries deemed higher risk and subject to monitoring reports or periodic reviews by the ILO, UN Human Rights Office, UN Environment Program or other relevant international organisations;

(g) Countries that have not ratified relevant international conventions and translated them into law.

6) **Sector risk factors:** Sector risks are risks that are prevalent within a sector globally as a result of the characteristics of the sector, its activities, its products and production processes.

For example:

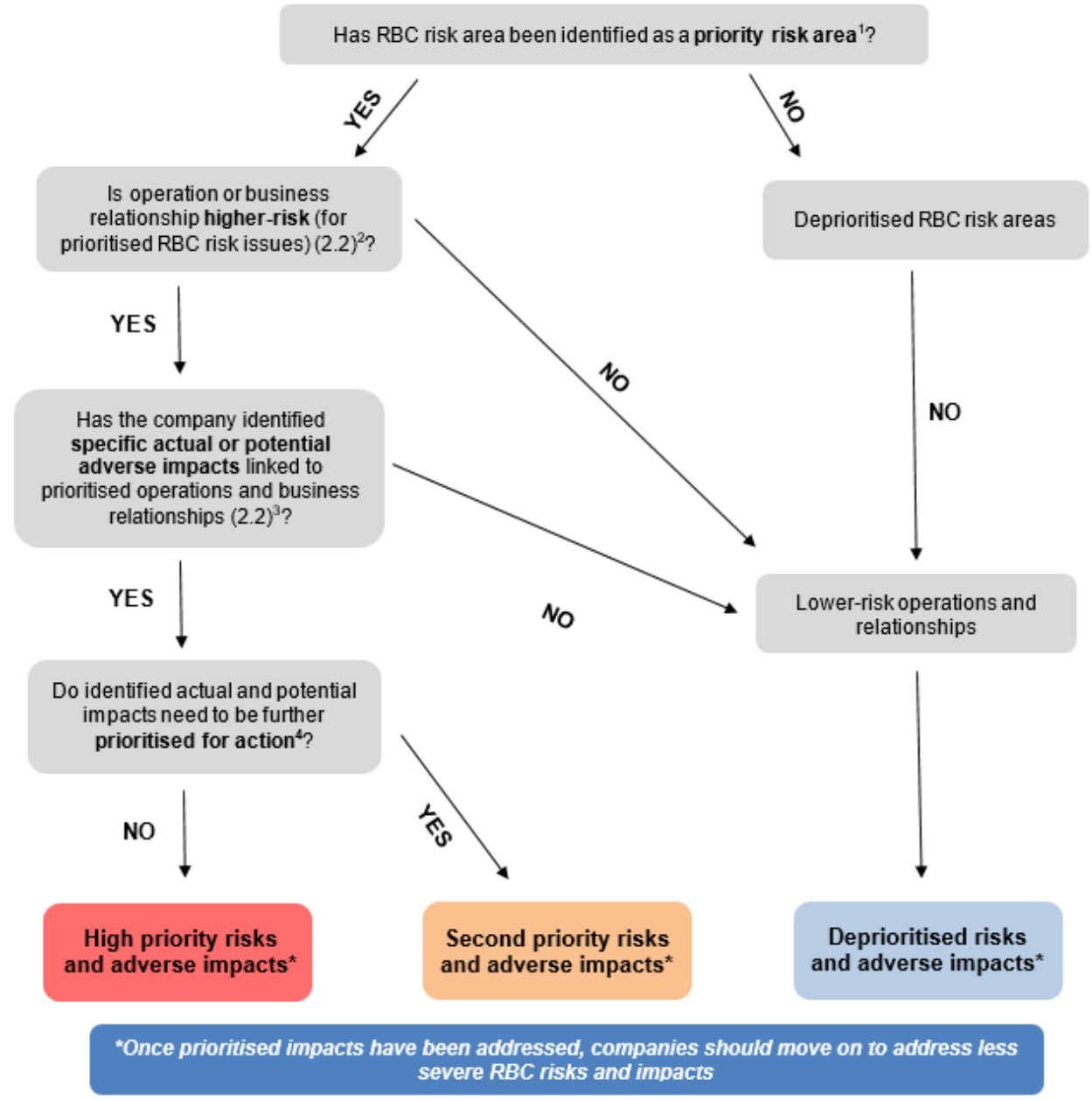
(a) Sectors that are inherently dangerous in their production or manufacturing, processes or that rely on low wage, informal or precarious work;

(b) Sectors associated with land grabs, or adverse impacts on land tenure rights and access to natural and cultural resources, including impacts on lands and natural resources subject to traditional ownership or under customary use, and other adverse impacts on indigenous peoples;

(c) Sectors that are widely associated with severe adverse human rights impacts, such as harassment, sexual and gender-based violence, discrimination, overtime, low wages or forced labour, or the misuse of data in an area that can adversely affect human rights or incentivise, cause, contribute to human rights abuses.

Annex B. Prioritising impacts for action

Figure A B.1. Examples of how enterprises should prioritise adverse impacts



Notes:

[1] Carry out a broad, high level scoping across operations and types of business relationships to prioritise most significant RBC risk areas on the basis of severity and likelihood of harm, taking into consideration "risk factors" (2.1). Update risk scoping with new information whenever the enterprise makes significant changes or engages in new forms of business relationships (2.1).

[2] Starting with prioritised RBC risk areas, carry out mapping and increasingly in-depth risk assessments of prioritised operations and business relationships to identify specific actual and potential adverse impacts.

[3] Assess the nature and extent of specific actual and potential impacts linked to prioritised operations and business relationships. Reassess impacts at regular intervals in accordance with Step 2.2.

Notes

[1] Black, J. (2010), "Risk-based Regulation: Choices, Practices and Lessons Being Learnt", in Risk and Regulatory Policy: Improving the Governance of Risk, OECD Publishing, Paris, https://www.oecd-ilibrary.org/governance/risk-and-regulatory-policy/risk-based-regulation_9789264082939-11-en.

[2] This policy note is not intended to provide a comprehensive analysis or summary of existing risk-based legislation, but rather draws from a selection of examples that can assist policy makers to address the questions raised.

[3] The OECD Guidelines for Multinational Enterprises (2011), OECD Due Diligence Guidance for RBC (2018) and sector-specific due diligence guidance, available at: http://mneguidelines.oecd.org/duediligence/.

[4] For example, the OECD Guidelines for Multinational Enterprises clarify that where "enterprises have large numbers of suppliers, they are encouraged to identify general areas where the risk of adverse impacts is most significant and, based on this risk assessment, prioritise suppliers for due diligence". See also OECD Due Diligence for RBC, Introduction and Annex, Q3 to Q5.

[5] See examples of indicators of scale, scope and irremediable character in the RBC Due Diligence Guidance, Table 3, p.43-44.

[6] Severity is not an absolute concept and is context specific. For examples of indicators of scale, scope and irremediable character across adverse impacts covered by the OECD Guidelines for MNEs, see OECD Due Diligence Guidance for RBC (2018), Table 3. These indicators are illustrative and will vary according to an enterprise's operating context.

[7] OECD, ILO, IOM, UNICEF (2019) Ending child labour, forced labour and human trafficking in global supply chains https://mneguidelines.oecd.org/ending-child-labour-forced-labour-and-human-trafficking-in-global-supply-chains.htm

[8] Choke points are key points of leverage in complex value chains that allow for companies further downstream to more effectively conduct due diligence in upstream segments of their value chains.

[9] The OECD Due Diligence Guidance for RBC provides examples of sector, product, geographic and enterprise-level risks (see Step 2.1 and Annex, Q20). Sectoral Due Diligence Guidances provide more detail on specific sector risks.

[10] The OECD Due Diligence Guidance for RBC sets out a definition of meaningful stakeholder engagement. See Annex, Q.9.

[11] For example, OECD Due Diligence Guidance for RBC, "key characteristics", Overview, p. 18 and Annex, Q8 to Q11.

[12] OECD Due Diligence Guidance for RBC (2018), Step 2.2, Measure (g).

[13] For example, see the OECD Due Diligence Guidance for Responsible Supply Chains in the Garment and Footwear Section, Section II, Modaules on sector risks which set out different expectations for tailored risk assessments and prevention and mitigation activities depending on the risk in question.

[14] See Step 6 of the OECD Due Diligence Guidance for RBC and Annex, Q. 29, p.70 for definitions of cause, contribute and direct linkage.

[15] OECD MNE Guidelines, Commentary on General Policies, Para 21 and OECD Due Diligence Guidance for RBC, Step 3.2 and Annex, Q34-40.

[16] See the OECD Due Diligence Guidance for RBC, Overview of Due Diligence, p. 18.

[17] Examples of existing due diligence legislation that integrates elements of a risk-based approach, to varying degrees and with different degrees of granularity include: France's LOI n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre of the French Commercial Code (Loi de Vigilance (2017)) : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034290626/ ; Germany's Act on Corporate Due Diligence in Supply Chains (2021) : https://www.bmas.de/EN/Services/Press/recent-publications/2021/act-on-corporate-due-diligence-in-supply-chains.html; Norway's Act relating to enterprises' transparency and work on fundamental human rights and decent working conditions (Transparency Act), 2021 (unofficial translation): https://www.regjeringen.no/contentassets/c33c3faf340441faa7388331a735f9d9/transparency-act-english-translation.pdf; and EU Regulation 2017/821 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas: https://policy.trade.ec.europa.eu/development-and-sustainability/conflict-minerals-regulation_en

[18] See Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing, Section 13, Article 18 and Articles 19-24. Available at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en

[19] See the definition of "model supply chain policy" and Article 4 of EU Regulation 2017/821 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:130:FULL&from=EN

[20] European Commission Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of EU Regulation 2016/679, 2017, https://ec.europa.eu/newsroom/article29/items/611236

[21] EU General Data Protection Regulation 2016/679, Article 35: https://gdpr-info.eu/art-35-gdpr/

[22] See Norwegian Transparency Act, 2021 (unofficial translation), Section 4: transparency-act-english-translation.pdf (regjeringen.no)

[23] The French Constitutional Council ruled that the initial draft of the law (more precisely the inclusion of the €10 million fine) was partially unconstitutional and in breach of the constitutional principle of "Principe de légalité" (or due process). The Court highlighted the vagueness and broad definitions of the obligations embedded in the due diligence process, including the substantial scope of risks (broad definition of human rights and fundamental liberties) the absence of strict interpersonal scope delimitation (business relationships and operations within scope) and vague character of "reasonable due diligence measures". As the result, the Constitutional Council ruled that the civil fine was deemed unconstitutional as it was sanctioning insufficiently defined obligations.

[24] EU General Data Protection Regulation 2016/679, Article 24(1): https://gdpr-info.eu/art-24-gdpr/

[25] See https://www.homeaffairs.gov.au/criminal-justice/files/modern-slavery-reporting-entities.pdf

[26] Guidance published by the German competent authority on risk assessments and prioritisation (2022), available at (in German only): https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bafa.de%2FSharedDocs%2FDownloads%2FDE%2FLieferketten%2Fhandreichung_risikoanalyse.pdf%3F__blob%3DpublicationFile%26v%3D3&data=05%7C01%7CEmily.NORTON%40oecd.org%7C2f08cd4c282640c40a4e08da87560a86%7Cac41c7d41f61460db0f4fc925a2b471c%7C0%7C1%7C637971100865353736%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=WX%2BK1vMphsEgNr0yJo5UxBggzjpNgTUcyyS4glpselA%3D&reserved=0

[27] These include “risks presented by the country and industry sector, the business opportunity, potential business partners, level of involvement with governments, amount of government regulation and oversight, and exposure to customs and immigration in conducting business affairs”. See: https://www.justice.gov/criminal-fraud/file/1292051/download

[28] https://gdpr-info.eu/. See Article 35: https://gdpr-info.eu/art-35-gdpr/

[29] Financial Action Taskforce Recommendations 2012 (amended March 2022): https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[30] Recommendations 1 and 10, including Interpretative Notes. Recommendation 10 states that the customer due diligence requirements “apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.”

[31] FATF Recommendations (2012), Interpretative note to Recommendation 1. See also Interpretative Note to Recommendation 10.

[32] FATF Recommendations, Interpretative Note to Recommendation 10.

[33] For example, in relation to politically exposed persons, correspondent banking, money or value transfers, new technologies and wire transfers, and higher-risk countries (see FATF Recommendations 12-16 and 18-19).

[34] FATF Recommendations, Interpretative Note to Recommendation 1.

[35] FATF Recommendations, Interpretative Note to Recommendation 10.

[36] FATF Recommendations, Interpretative Note to Recommendation 10.

[37] The EU’s 4th Anti-Money Laundering Directive (EU) 2015/849 has since been amended by Directive (EU) 2018/843 (5th Anti-Money Laundering Directive) which tightens the EU’s rules, extends to scope of the directive and enhances cooperation between Financial Intelligence Units. Directive (EU) 2019/2177 further amends Directive (EU) 2015/849 to take into account amendments made to Regulation (EU) No 1093/2010 setting up the European Banking Authority (see summary).

[38] Chapter II of the Directive, including Section 1, ‘General provisions’, Section 2, ‘Simplified customer due diligence’, Articles 15-17 and Section 3, ‘Enhanced customer due diligence’, Article 18-24.

[39] Article 13(3) and Annex I.

[40] European Supervisory Authorities (EBA, EIOPA and ESMA), ‘Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions’ (Risk Factors Guidelines), 2017.

[41] For example, see Centre for Information Policy Leadership, Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (2016), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

[42] For more information on meaningful stakeholder engagement, see OECD Due Diligence Guidance for RBC (2018), Annex, Q9.

[43] See section 4(4) and section 9 of the German Supply Chain Act (2021): https://www.bmas.de/EN/Services/Press/recent-publications/2021/act-on-corporate-due-diligence-in-supply-chains.html

[44] See Recommendation 10 to the FATF Recommendations (2012).

[45] EU’s 4th Anti-Money Laundering Directive (2015/849). See, for example, Chapter II, Customer Due Diligence, Section 1, Article 13 and Article 20.

[46] https://www.homeaffairs.gov.au/criminal-justice/files/modern-slavery-reporting-entities.pdf

[47] EU's 4th Anti-Money Laundering Directive (2015/849). See Chapter II, Customer Due Diligence, Section 1, Article 13(2).

[48] EU's 4th Anti-Money Laundering Directive (2015/849), Chapter II, Customer Due Diligence, Section 3, Article 18.

[49] See Article 24 of the EU General Data Protection Regulation (2016/679).

[50] See Section 6 of the German Supply Chain Act (2021): https://www.bmas.de/EN/Services/Press/recent-publications/2021/act-on-corporate-due-diligence-in-supply-chains.html

[51] The UN Guiding Principles, OECD MNE Guidelines and OECD Due Diligence Guidances differentiate responsibilities for companies depending on whether they have caused, contributed to or are directly linked to an actual adverse impact (or may cause, contribute to or be directly linked to a potential adverse impact). See Steps 3 and 6 of the six-step due diligence framework in the OECD Due Diligence Guidance.

[52] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1040283/Transparency_in_Supply_Chains_A_Practical_Guide_2017_final.pdf

[53] See Interpretative Note to Recommendation 1: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[54] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 2017: https://ec.europa.eu/newsroom/article29/items/611236/en

[55] European Commission, 'Guidelines on Transparency under Regulation 2016/679', 2018: https://ec.europa.eu/newsroom/article29/items/622227/en

[56] See OHCHR, Interpretative Guide to the United Nations Guiding Principles. See: https://www.ohchr.org/sites/default/files/Documents/publications/hr.puB.12.2_en.pdf