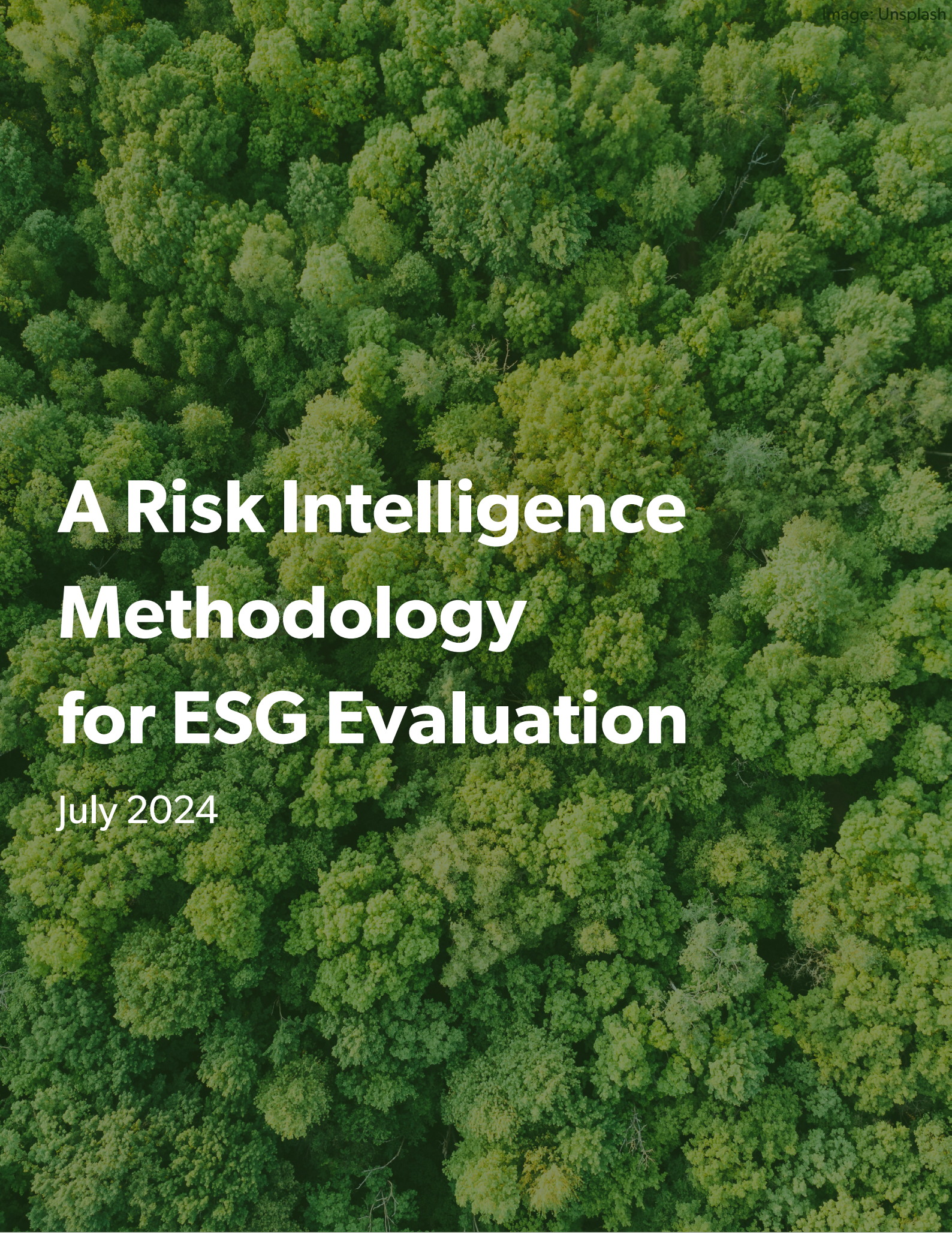

Image: Unsplash

A Risk Intelligence Methodology for ESG Evaluation

July 2024

PRINCEPS
RISK INTELLIGENCE INSTITUTE

Iceland Liechtenstein Norway grants

Norway grants

Prios

This document was produced as part of the bilateral project
"Designing a Risk Intelligence Methodology for ESG evaluation" managed by the
PRINCEPS Risk Intelligence Institute (CZ) and Prios Kompetanse (NO).
The project is funded by EEA Norway Grants 2014-2021.

You can learn more about the project at **princepsinstitute.com/esgmethodology**.

Contents

1. Introduction & Rationale

The concept of ESG (environmental, social, and governance) has firmly embedded itself in mainstream business and political discourse. The emphasis on ethical conduct in environmental, social, and governance matters is more than a mere buzzword; a 2023 survey of executives across industries conducted by EY revealed that 87% of all respondents believed ESG initiatives to be "very to extremely important".[1] Furthermore, PwC reports that 75% of employees list the overall societal impact of a company as an important factor when selecting an employer, followed by the company's environmental policies and practices (68.6%) and governance policies (66.7%).[2]

For most businesses, the key motivation for ESG reporting and assessment is risk management; the findings of BNP Paribas indicate that regulatory (60%) and reputational (58%) risks are major drivers behind investors' assessments of potential investment opportunities.[3] The aforementioned research also highlights the importance of ESG initiatives and reporting for managing internal risks related to company culture and operations, employee satisfaction and retention, and adaptation to the contemporary business environment while creating opportunities for value creation.

While ESG evaluations and reporting present the most straightforward path towards managing ESG-related risks, they remain limited by the availability and management of data. Commonly reported ESG metrics include carbon emissions (used by 56% of respondents in 2023), diversity statistics (24%), and impact metrics with SDG alignment (17%), all of which provide significantly limited and decontextualised information. Alternatively, 37% of respondents report externally derived ESG scores.[4] These provide aggregate markings, often without disclosing the precise methodology involved, and reveal little about the standards of individual ESG categories, the relevant issues, and their localisation. Reporting thus becomes primarily performative and loses the ability to inform and drive sustainable change.

---

1 'EY Survey: Executives' Views on Sustainability & ESG', 2023, https://www.ey.com/en_us/sustainability/sustainability-and-esg-trends-index.

2 'ESG Worker Preferences Study | PwC', 2024, https://www.pwc.com/gx/en/issues/workforce/pwcs-global-workforce-sustainability-study.html.

3 'Global ESG Survey 2023 - Securities Services', 2023, https://securities.cib.bnpparibas/global-esg-survey-2023/#survey-summary.

4 '2023 Manager ESG Survey: Key Insights | Russell Investments', accessed 24 July 2024, https://russellinvestments.com/uk/blog/2023-esg-manager-survey.

In 2022, the European Union published its Corporate Sustainability Reporting Directive (CSRD), which requires some fifty thousand businesses listed and/or operating in the EU to regularly report on their sustainability performance. The CSRD intends to drive change in business conduct by mandating the analysis of issues such as climate change, loss of biodiversity, and human rights, relating them to the company's opportunities, risks, and impacts, and disclosing strategies and plans for their improvements.[5] Understandably, "one size fits all" metrics cannot provide the information necessary for businesses to comprehensively address outstanding ESG issues. However, their acceptance simultaneously fails to create incentives to actively problematise and incorporate ESG factors into their everyday business cultures.

We present the Risk Intelligence Methodology for ESG Evaluation as a response to the limitations of mainstream ESG scoring outlined above. Risk intelligence provides companies with a highly customisable approach to information, which can be managed internally and integrated into companies' regular business operations. Its focus lies on complex qualitative evaluation, which leads both to the identification of outstanding issues and their far-reaching impact. By applying risk intelligence approaches to ESG assessment, we hope to empower companies to take control of their own ESG reporting to comply with regulatory requirements, as well as to identify outstanding issues and their impacts and highlight how they can be addressed.

5 Eu-Lin Fang et al., 'The CSRD Is Resetting the Value-Creation Agenda', PwC, 2023, https://www.pwc.com/gx/en/issues/esg/csrd-is-resetting-the-value-creation-agenda.html.

2. Risk Intelligence Overview

We begin by providing a general overview of risk intelligence as an approach and the main types of risks it addresses. The following section then explains how risk intelligence operates as a method for identifying, assessing, mitigating, and monitoring risks. We continue by introducing stakeholder mapping as an alternative risk management strategy to risk intelligence. We conclude by identifying how and why risk intelligence can provide a meaningful addition to ESG reporting and evaluations. Risk intelligence is an umbrella term for a discipline that, at its core, focuses on collecting, processing, and analysing information to understand and mitigate risks, reduce uncertainty, and support business leaders in making informed strategic decisions.

Risk intelligence processes, techniques, and tools are widely used in more narrowly defined and focused disciplines that collectively fall under its umbrella, such as non-financial due diligence and insider threat investigations. Furthermore, its outputs have been utilised by associated fields such as compliance, business intelligence, and forecasting, among others. Its wide range and applicability lend themselves to new and emerging challenges, including requirements for comprehensive sustainability assessments.

Risks & Uncertainty

Under its umbrella, risk intelligence encompasses multiple types of risk, including, but not limited to, political, reputational, regulatory, and market risk. The following sections outline the characteristics and potential impacts of each category.

Political Risk

Political Risks are risks stemming from political events, activities, or decisions, which negatively impact businesses, governments, and investors. These risks can have a significant influence on the resources, operations, or profitability of an organisation. Political risks can derive from government policies or regulations, as well as from political unrest such as riots, terrorism, or conflict.

Changes in government policies, such as new financial regulations, trade restrictions, or asset nationalisation, can directly affect the financial stability and operational efficiency of a company. These regulatory changes might require businesses to alter their practices, leading to increased

costs or reduced competitiveness. Additionally, political instability, including protests, strikes, and violent conflicts, can disrupt supply chains, interrupt day-to-day operations, and damage assets, thus hindering business activities.

For investors, political risks can lead to sudden changes in market conditions, affecting investments or assets. Governments facing economic difficulties might choose to expropriate foreign-owned assets, posing a direct threat to investments. Multinational companies, in particular, must navigate these risks across different regions, making political risk assessment a crucial component of their strategic planning.

Understanding political risks is essential for maintaining operational resilience and making long-term strategic business decisions. In order to understand political risks, companies often employ advisory firms that research and assess relevant risks and evaluate their potential to hurt a company's assets or investments.

Reputational Risk

A reputational risk is a form of risk in which a company or an entity faces a potential loss of financial capital, social capital, and/or market share due to actions or information leading to a negative public perception. This type of risk can arise from various sources, including unethical behaviour, potentially criminal conduct, negative media coverage, or associations with entities involved in such conduct. The damage from reputational risks can cause companies to lose out on revenue, contracts, future business opportunities, or trust from other entities.

Reputational risks are often more severe than other types of risks because they directly affect the trust and confidence that stakeholders – such as customers, investors, or even employees – have in an organisation. For instance, a scandal involving a company's leadership can lead to investors exiting the company, the stock value decreasing, or a loss of trust from potential customers. Similarly, negative media coverage can amplify public scrutiny and result in a broader reputational crisis.

The rise of social media has made managing reputational risks even more challenging, as information is being shared more rapidly and widely. A single negative incident can quickly escalate, affecting a company's image globally. To mitigate reputational risks, businesses must maintain

high-level ethical standards, ensure transparent communication, and engage in proactive reputation management strategies, such as in-depth due diligence of the parties they engage with. By actively managing its reputation, a firm can protect its brand and sustain its market position.

Regulatory Risk

Regulatory risks arise from changes in legislation, regulations, or policies that can negatively impact businesses, governments, and investors. Regulatory risks can stem from the introduction of new legislation, amendments to existing regulations, or more stringent enforcement practices by governmental bodies. These risks can lead to challenges to an organisation's assets, disrupt its operations, and affect overall financial performance. For example, new environmental regulations and their subsequent increased demands for ESG compliance might necessitate costly modifications to production processes. Regulatory risks can also arise from international policies, such as trade tariffs or sanctions, which can disrupt supply chains or limit market access. The impact of these risks is often compounded for multinational companies operating in multiple jurisdictions, each with its regulatory landscape.

The damage from regulatory risks can cause companies to lose out on revenue, incur fines, face legal challenges, or suffer from operational disruptions. To mitigate these risks, businesses ought to stay informed about potential regulatory changes, engage in active advocacy, and develop flexible strategies that allow for quick adaptation to new legal environments.

Market Risk

Market risks arise when entering a new market, such as local competition pressure, existing regulatory obstacles, cases of corruption, and supply chain challenges. Furthermore, companies may face challenges when navigating unfamiliar regulatory landscapes, cultural differences, and the need to establish a new customer base. The unpredictability of market demand and the presence of established competitors can further complicate market entry.

To mitigate market risks, businesses conduct thorough market research, develop flexible strategies, and maintain robust risk management and mitigation practices. By understanding and preparing for these potential challenges, companies can better navigate the complexities of the market and safeguard their finances and operations by reducing uncertainties.

In today's globalised world, however, these risks no longer exist individually in predefined lists but are instead interconnected and influenced by one another. What they do have in common is the underlying uncertainty. While it is unfeasible to remove uncertainty from the picture entirely, risk intelligence provides the steps to comprehensively and continuously mitigate uncertainty and its adverse effects on business operations.

3. A Risk Intelligence Methodology

The risk intelligence approach to reducing uncertainty consists of four steps:

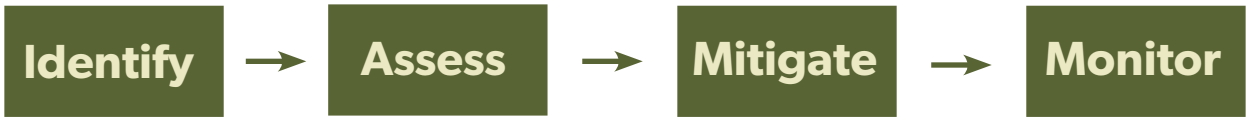

Diagram: Risk Intelligence Methodology

Identify

The first and crucial step in reducing uncertainty is the concrete identification of risks that may influence business operations and strategic decision-making. The key component of this step is to establish a relevant research scope by formulating suitable guiding questions that define the known knowns and the known unknowns. For example, when considering the risks associated with the value chain, businesses have to first understand what actors make up their upstream and downstream value chain. While businesses may know who their primary suppliers and customers are, additional research may be required to also identify any associated third-party suppliers, support organisations, resellers, etc. to address the relevant risks comprehensively.

The establishment of the scope is followed by the collection and processing of relevant data. Here, risk intelligence generally utilises the best practices of two collection methods known as human intelligence (HUMINT) and open-source intelligence (OSINT). As the name suggests, HUMINT relies on collecting information from human sources through passive observation and/or active interaction with people, while OSINT relies on collecting, processing, and analysing information from publicly available and legal sources. Such sources may include public government data, news, blogs, social media, grey literature, and the dark web, but also print media, books, and other physical publications.

Regardless of the collection method, stakeholders must consider both the reliability of the source and the credibility of the information it provides. Reliability can be assessed based on the track record of the information sources. For example, human sources may be considered reliable if their competence matches the required expertise and experience. Credibility is then often assessed based on the ability of the information to be verified from other sources. For example, peer-reviewed and highly cited articles and books are often considered among the most credible sources. Once relevant information has been collected, it is possible to highlight the specific areas of exposure and consider potential threats.

Assess

The process of assessing the identified risks must begin with a self-assessment of the company's risk appetite. Defined as the amount and type of risk a business is willing to pursue or retain, understanding the risk appetite will determine what actions, if any, are necessary to mitigate the risks. Risk appetite will differ for every business based on multiple internal and external aspects. Internal aspects may include factors such as personality traits and experiences of the decision-makers or the overall company culture. External aspects then may include the type of industry and competitors. For example, a leadership that was forced to close their operations in one country following authoritarian backsliding and nationalisation of the industry may be more risk averse when dealing with political risks. As a result, they may avoid opening operations in a country that is assessed as unstable.

Once the business has defined its risk appetite, it should evaluate the probability and potential impact of the identified risks. These two qualities both determine the severity of the risk, as outlined by the probability and impact matrix. The severity of the risk increases with its likelihood and the severity of its impact. We provide a more detailed discussion of both factors below.

Note that while the use of risk matrices is a common risk management strategy, they should be viewed as a reference tool and a framework for discussion rather than the final answer to risk assessment.

<u>Risk Probability</u>

There are two approaches to assessing risk probability and thus locating the risk on the probability scale: quantitative and qualitative assessment.

The quantitative approach takes advantage of hard measurable data and is often expressed in percentages, ratios, and other quantifiable findings. The main issue when using quantitative approaches may be the unavailability or limited scope of the necessary data. Alternatively, the qualitative approach consists of a comprehensive assessment of available information, which cannot be expressed numerically. This includes but is not limited to the evaluation of textual information, such as academic, journalistic and other publications, observation, and interview responses. The findings are then located on a predefined scale, for example:[6]

1 – Very unlikely: A very slim chance for this risk to occur.
2 – Not likely: Low chances for this risk to occur.
3 – Possible: Fifty-fifty chances for this risk to occur.
4 – Probable: Good chances for this risk to occur.
5 – Very likely: You can bet this risk will occur at some point.

Impact
How severe would the outcomes be if the risk occurred?

Probability
How likely is the risk to occurr?

	Negligible	**Low**	**Moderate**	**Significant**	**Catastrophic**
Very likely	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
Not likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
Possible	Low 3	Medium 6	Medium 9	High 12	Very high 15
Probable	Very low 2	Low 4	Medium 6	Medium 8	High 10
Very unlikely	Very low 2	Very low 2	Low 3	Medium 4	Medium 5

Diagram: Probability and Impact

Successful qualitative evaluation relies on deep knowledge of the context in which the risk may occur to avoid one-sided or misleading conclusions.

6 'ISO Guide 73:2009(En), Risk Management — Vocabulary', accessed 24 July 2024, https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

While the quantitative approach may at first glance appear more scientific, both approaches rely on subjective choices made by the researcher and thus cannot be approached as bulletproof. Indeed, much like in the case of qualitative evaluation, the selection of data for quantitative analysis also consists of a personal choice made by the researcher, which can be impacted by their biases in opinion and limited information. A comprehensive understanding of the context is therefore necessary in both cases to effectively discern which information is credible and relevant to the assessment.

Risk Impact

The impact scale describes the potential consequences or effects that may result from the occurrence of a specific risk. Typically, risk impact is once again expressed on a scale, such as the following:

1 – Negligible: This risk will hardly impact your project.
2 – Low: You can easily handle the consequences of this risk.
3 – Moderate: It will take some time and effort to mitigate the consequences of this risk.
4 – Significant: This risk could cause long-term consequences that will be hard to recover from.
5 – Catastrophic: The impact of this risk might wreck your project

Similar to the probability scale, the impact scale can also be expressed in quantitative terms – a common approach is choosing to express the impact in terms of financial losses. Most importantly, businesses should customise the impact scale and the specific consequences to apply to the circumstances of their organisation and its context.

Risk Rating

After establishing the probability and impact scales and assigning their values to different risk events identified in the previous step, the resulting risk rating is calculated according to the risk matrix above.

Risk Probability X Risk Impact = Risk Rating

An example of different approaches to assessing risk probability:[7]

Qualitative Likelihood	Historical Occurences	Natural Frequencies	Probability
Is expected to occur in most circumstances	Has occurred on an regular basis in the organization during the timeframe or circumstances are in train that will cause it to happen.	Is likely, or has been known to occurr 90 times every 100 timeframes.	0.90 (0.81-0.99)
Will probably occurr in most circumstances	Has occurred in the organization within 3 multiples of the timeframe being considered.	Is likely, or has been known to occur roughly 70 times in 100.	0.70 (0.61-0.80)
Might occur at some time	Has occurred previously in the history of the organization and/or in other similar organizations or circumstances.	Is likely, or has been known to occur approximately 50 out of 100 times.	0.50 (0.41-0.60)
Could occur at some time	Has never occurred in this organization but has occurred infrequently in other similar organizations.	Is likely, or has been known to occurr less than 1 in 10,000 times.	0.30 (0.21-0.40)
Can only occurr in exceptional circumstances	Is possible but has not occurred to date in this or any similar organizations.	Is likely, or has been known to occurr less than once in 100 timeframes.	0.10 (0.01-0.20)

7 Adapted from Julian Talbot, "*Security Risk Management: Aide-Mémoire*" (2019): 96.

Using the 5 x 5 scale illustrated in the previous subsections, the risk rating may look like this:[8]

1 – 6 Low: Low-rating risks will most likely not happen. If they do, they will not be a threat to your organisation.
7 – 12 Medium: Some medium-rating risks might occur at some point. You do not need to prioritise them, but you should not ignore them, either.
13 – 25 High: High-rating risks are serious threats that are very likely to happen. They can seriously impact the operations and health of your organisation and ought to be addressed accordingly.

Given that mitigating and managing risks requires resources, consulting the probability and impact matrix allows stakeholders to identify the most critical risk categories and create a list of priorities their risk mitigation and management efforts should focus on. While nearly every organisation will (or ideally should) take steps to address the risks identified in the highest rating, the approach to the other identified risks will typically depend on the organisation's risk appetite and available resources. These conscious decisions in aligning strategy and risk are sometimes referred to as the "risk appetite framework".[9]

Mitigate

After identifying the risks and assessing their impact and likelihood of occurrence, stakeholders now must consider their options for mitigating them. As stated above, the type of risks and mitigation strategies will depend on the organisation's risk appetite and available resources. Generally, stakeholders may consider the following options for mitigating risks:[10]

- Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk.
- Remove the risk source.
- Change the probability.
- Change the impact.
- Share the risk (e.g. through contracts, insurance, etc.) to distribute its impact.
- Retain the risk by informed decision (typical for less significant risks).

8 Agnieszka Sienkiewicz, 'Project Risk Assessment: An Example with a Risk Matrix Template', BigPicture, 2022, https://bigpicture.one/blog/project-risk-assessment-examples/.
9 'Using a Risk Appetite Framework to Align Strategy and Risk', 2015, https://www.moodys.com/web/en/us/insights/banking/using-a-risk-appetite-framework-to-align-strategy-and-risk.html.
10 Talbot, *Security Risk Management Aide-Mémoire*, 117.

- Take or increase the risk to pursue an opportunity (typical for high risks with high rewards).

An example of different approaches to assessing risk impact.[11]

PEOPLE	Minor injury or first aid treatment.	Injury requiring treatment by medical practitioner and/ or lost time from workplace.	Major injury/hospitalisation.	Single death and/ or multiple major injuries.	Multiple deaths.
INFORMATION	Compromise of information otherwise available in the public domain.	Minor compromise of information sensitive to internal or sub-unit interests.	Compromise of information sensitive to organisational interests.	Compromise of information sensitive to organisational interests.	Compromise of information with significant ongoing impact.
PROPERTY	Minor damage or vanadalism to asset.	Minor damage or loss of <5% of total assets.	Damage or loss of <20% of total assets.	Extensive damage or loss of approx. 50% of total assets.	Destruction or complete loss of >50% of assets.
ECONOMIC	1% of budget or revenue (organizational, division or project budget as relevant).	10-20% of budget.	40-60% of budget or revenue.	60-80% of budget or revenue.	>80% of project or organisational budget or revenue.
REPUTATION	Local mention only. Quickly forgotten.	Scrutiny by Executive, internal committees or internal audit to prevent escalation. Short term local media concern. Some impact on local level authorities.	Persistent national concern. Scrutiny required by external agencies. Long term "brand" impact	Persistent intense national public, political and media scrutiny.	International concern. Governmental Inquiry or sustained adverse national/international media. "Brand" significantly affects organisational abilities.
CAPABILITY	Minor skills impact. Minimal impact on non-core operations. The impact can be dealt with by routine operations.	Some impact on organizational capability in terms of delays, systems quality but able to be dealt with at operational level.	Impact on the organisation resulting in reduced performance such that targets are not met. Organisation's existence is not threatened, but could be subject to significant review.	Breakdown of key activities leading to reduction in performance (eg. service delays, revenue loss, client dissatisfaction, legislative breaches).	Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/ organisation is threatened.

11 Adapted from Talbot, *Security Risk Management Aide-Mémoire*, 117.

When considering their choice of risk mitigation strategies, stakeholders should keep in mind the "4As" model:[12]

- Appropriate: Addresses the root cause.
- Actionable: Specific timeframes, actions, resources, and accountable personnel to implement the treatment/recommendation.
- Achievable: Criteria, individual judgement, or milestone by which the recommendation will be considered complete.
- Agreed: Relevant personnel were consulted and supported the decision.

Monitor

Establishing strategies and approaches to risk mitigation is not the last step in reducing uncertainty. Instead, stakeholders should set up indicators for each of the identified risks and establish specific monitoring steps and strategies based on the organisation's needs. A key component of monitoring is to identify the early indicators that may alert the stakeholders to an impending risk.

For example, a business operating in a democratic country with a stable government might only monitor the local political situation before major elections. On the other hand, a business operating in a semi-autocratic country that has been dropping in the human freedom index rankings may require more complex and frequent monitoring.

The scope of monitoring and utilised sources and methods will vary based on the identified risks, risk appetite, and mitigation strategies. Typically, businesses may monitor the situation using local news sources, relevant indices established by various governmental and non-governmental organisations, regular subject-matter studies, and the help of local subject-matter expert organisations.

12 Talbot, Security Risk Management Aide-Mémoire, 119.

4. Stakeholder Mapping

The methodology outlined above that relies on identifying, assessing, mitigating, and monitoring risks is one way of reducing uncertainty. A different approach widely utilised by risk intelligence professionals is to identify key individuals and groups with the knowledge or influence necessary to impact specific issues or policies that already do or may affect the organisation.

While stakeholder mapping could be considered part of the "Identify" step in the previous section, its goal is not to describe risks, but instead to mitigate them directly by ultimately developing relationships and engaging with these stakeholders to gain advanced knowledge. As such, it deserves special attention. It is also helpful to consider stakeholder mapping as an addition to the risk intelligence methodology outlined above, rather than its alternative outright.

For organisations looking to effectively navigate the political landscape and further their interests, stakeholder mapping is essential. By systematically identifying relevant stakeholders, businesses can better understand the contextual environment, anticipate potential challenges, and leverage opportunities to influence policy outcomes.

Various processes are involved in the political stakeholder mapping process. First, it requires a comprehensive analysis of the political context in which the organisation operates, including identifying key issues that might affect the company's operations or strategic goals. Second, organisations must identify and select the stakeholders with a significant impact on these issues. These stakeholders include government officials, policymakers, regulatory bodies, advocacy groups, and influential public figures. The objective is to discover and narrow down specific experts or other influential stakeholders who either have additional knowledge on particular issues or potential influence on policy decisions.

Once identified, these stakeholders are mapped and rated based on their level of influence and the feasibility of engaging with them. The feasibility of engagement is a function of both accessibility and reputational risks. For instance, former high-level politicians who are no longer in office may still have relevant connections and be willing to cooperate, but their association with various scandals would make working with them a reputational risk. This could mean that despite the stakeholder's accessibility and significance, association with them may not be

worth the reputational risk. Much like in the case of business risks, assessing the risk of engaging stakeholders may depend on the business' risk appetite. High-priority stakeholders are those with both high influence and high potential for engagement. Low-priority stakeholders are those who either have low influence on the given matter or are challenging/risky to engage with.

Effective stakeholder engagement involves building relationships through various means, such as direct communication, participation in relevant forums and conferences, or collaboration on mutual interests. By maintaining an ongoing dialogue with the stakeholders, businesses can stay informed about policy developments, advocate for their positions, and contribute to policy discussions.

5. Applied Approach to ESG Evaluation

Voluntary European Reporting Standards

The risk intelligence approach to identifying, assessing, mitigating, and monitoring risks can be especially useful to non-listed small and medium enterprises (SME) that are not (yet) required to report the standards set by the Corporate Social Reporting Directive.

Using this comprehensive approach has two benefits. First, non-listed SMEs can better understand the risks associated with failing to adopt some of the Voluntary European Sustainability Reporting Standards (VSME) and thus determine whether or not they should adopt them. Second, a better understanding of the risks facing their organisations allows the stakeholders to better shape their reporting under the VSME standard by addressing the most critical issues.

Customised Steps

Additionally, the individual steps from the methodology can be used for various needs associated with fulfilling the CSRD requirements. While the vast majority of the European Sustainability Reporting Standards (ESRS) look inside businesses and provide guidance on the collection and evaluation of internal data, policies, and processes, some of the arguably most critical requirements concern information from outside of businesses. Indeed, the emphasis on the entire value chain places pressure on businesses to properly map out and understand their value chain and the specific risks associated with each part of the chain.

This is especially important when considering the following reporting standards; ESRS S2: Workers in the Value Chain, ESRS S3: Affected Communities, and ESRS S4: Consumers and End--Users. For example, the ESRS S2, which aims to "understand material impacts on value chain workers," is a particularly challenging standard that may benefit from the risk intelligence approach.[13]

The general guidelines assume complete knowledge of the value chain. However, in reality, businesses often lack such knowledge, and when collecting information they typically have to rely on the data provided by the various actors along the chain.

Although businesses may be able to partially fulfil the reporting standards, they run the risk of omitting or misrepresenting crucial data and thus failing to correctly assess all relevant risks. The risk intelligence approach stresses the importance of conducting original research and collecting reliable and credible information. As such, it both supports fulfilling ESG standards, and, perhaps more importantly, it also sets up businesses for long term success.

For example, when evaluating the S2 standards, the non-negotiable prerequisite for their fulfilment is a complete understanding of the individual business' upstream and downstream value chain. Businesses must thus identify all the actors that are part of the chain, including direct actors who interact with them (e.g. their suppliers and customers) as well as indirect actors along the chain (e.g. third parties associated with the suppliers and resellers).

Therefore, businesses may ask the following general questions about their suppliers to guide their information gathering process:

a. Where is the supplier headquartered, and where does it have its main operations?
b. What is the supplier's corporate structure? Does it have any parent companies or subsidiaries?
c. Who are the beneficial owners of the supplier?
d. How long has the supplier been in business?
e. Who are the supplier's other major customers?
f. Who are the supplier's competitors?

13 'Draft European Sustainability Reporting Standards: ESRS S2 Workers in the Value Chain' (EFRAG, November 2022), https://www.efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FSiteAssets%2F14%25.

These general guiding questions touch on the types of risks discussed earlier. Questions a), b), and c) directly relate to political and regulatory risks, as the jurisdictions where they operate have direct impact on these categories. Questions d), e), and f) directly relate to market risk, and all questions relate to reputational risks. To illustrate further, a business may have a contract with a supplier that, per their mutual agreement, sells equipment parts manufactured in a jurisdiction that has no history of child and forced labour. However, the supplier's sister company has production factories in jurisdictions where such violations have occurred in the past.

Additionally, the supplier has in the past used the sister company to fulfil overflow orders without disclosing it to their customers. In this example, a mere reliance on the contract and disclosures from the supplier may satisfy some of the ESG requirements on paper but fail to properly identify the hidden risks which may negatively impact the business down the road.

6. Conclusion

The Risk Intelligence Methodology for ESG Evaluation presents a comprehensive, step-by-step approach to the risk intelligence method of sourcing and evaluating information.

The key advantage is the approach's customisability. One of our key aims is to provide organisations with a tool for independent information and risk management that can be seamlessly integrated into their everyday business operations without creating major financial and personal strain. By narrowing the focus of the research and guiding questions to ESG-related matters, risk intelligence can empower companies to conduct their own ESG evaluation leading to definable and actionable steps towards greater sustainability. This process is developed further in our Strategic Action Plan for SMEs, which builds on the Methodology by providing specific step-by-step guides to integrating risk intelligence methods into SMEs' reporting practices.

We hope both documents will empower companies to adapt the risk intelligence approach to suit their reporting needs and develop more robust and informed ESG practices.

References

'2023 Manager ESG Survey: Key Insights | Russell Investments'. Accessed 24 July 2024. https://russellinvestments.com/uk/blog/2023-esg-manager-survey.

'Draft European Sustainability Reporting Standards: ESRS S2 Workers in the Value Chain'. EFRAG, November 2022. https://www.efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FSiteAssets%2F14%2520Draft%2520ESRS%2520S2%2520Workers%2520in%2520the%2520value%2520chain%2520November%25202022.pdf.

'ESG Worker Preferences Study | PwC', 2024. https://www.pwc.com/gx/en/issues/workforce/pwcs-global-workforce-sustainability-study.html.

'EY Survey: Executives' Views on Sustainability & ESG', 2023. https://www.ey.com/en_us/sustainability/sustainability-and-esg-trends-index.

Fang, Eu-Lin, Peter Gassmann, Kevin O'Connell, and Nadja Picard. 'The CSRD Is Resetting the Value-Creation Agenda'. PwC, 2023. https://www.pwc.com/gx/en/issues/esg/csrd-is-resetting-the-value-creation-agenda.html.

'Global ESG Survey 2023 - Securities Services', 2023. https://securities.cib.bnpparibas/global-esg-survey-2023/#survey-summary.

'ISO Guide 73:2009(En), Risk Management — Vocabulary'. Accessed 24 July 2024. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

Sienkiewicz, Agnieszka. 'Project Risk Assessment: An Example with a Risk Matrix Template'. BigPicture, 2022. https://bigpicture.one/blog/project-risk-assessment-examples/.

Talbot, Julian. Security Risk Management Aide-Mémoire, 2019.

'Using a Risk Appetite Framework to Align Strategy and Risk', 2015. https://www.moodys.com/web/en/us/insights/banking/using-a-risk-appetite-framework-to-align-strategy-and-risk.html.

PRINCEPS Risk Intelligence Institute

PRINCEPS Risk Intelligence Institute is a Czech non-profit organisation dedicated to developing the risk intelligence industry standards in Central and Eastern Europe. PRII aspires to create a regional centre of excellence in risk intelligence that connects experts, executives, and young professionals. It likewise aims to establish a shared network, educational opportunities, and modern tools to navigate any current risk intelligence challenges.

www.princepsinstitute.com

Prios Kompetanse AS

Prios Kompetanse AS is a Norwegian nationally recognised centre for adult education and lifelong learning. Consulting activities mainly support Prios' clients with internal innovation processes, economic advice, ESG management, green innovations, circular economic development, and management improvements. As a research centre, Prios aims to implement the idea of lifelong learning and constantly updating training contents and methods in response to the ongoing digitalisation and developments of the business sector.

www.prios.no

Authors

The authors are members of the PRINCEPS Risk Intelligence Institute.

Image: Unsplash

PRINCEPS

RISK INTELLIGENCE INSTITUTE

Iceland Liechtenstein Norway grants

Norway grants

Prios