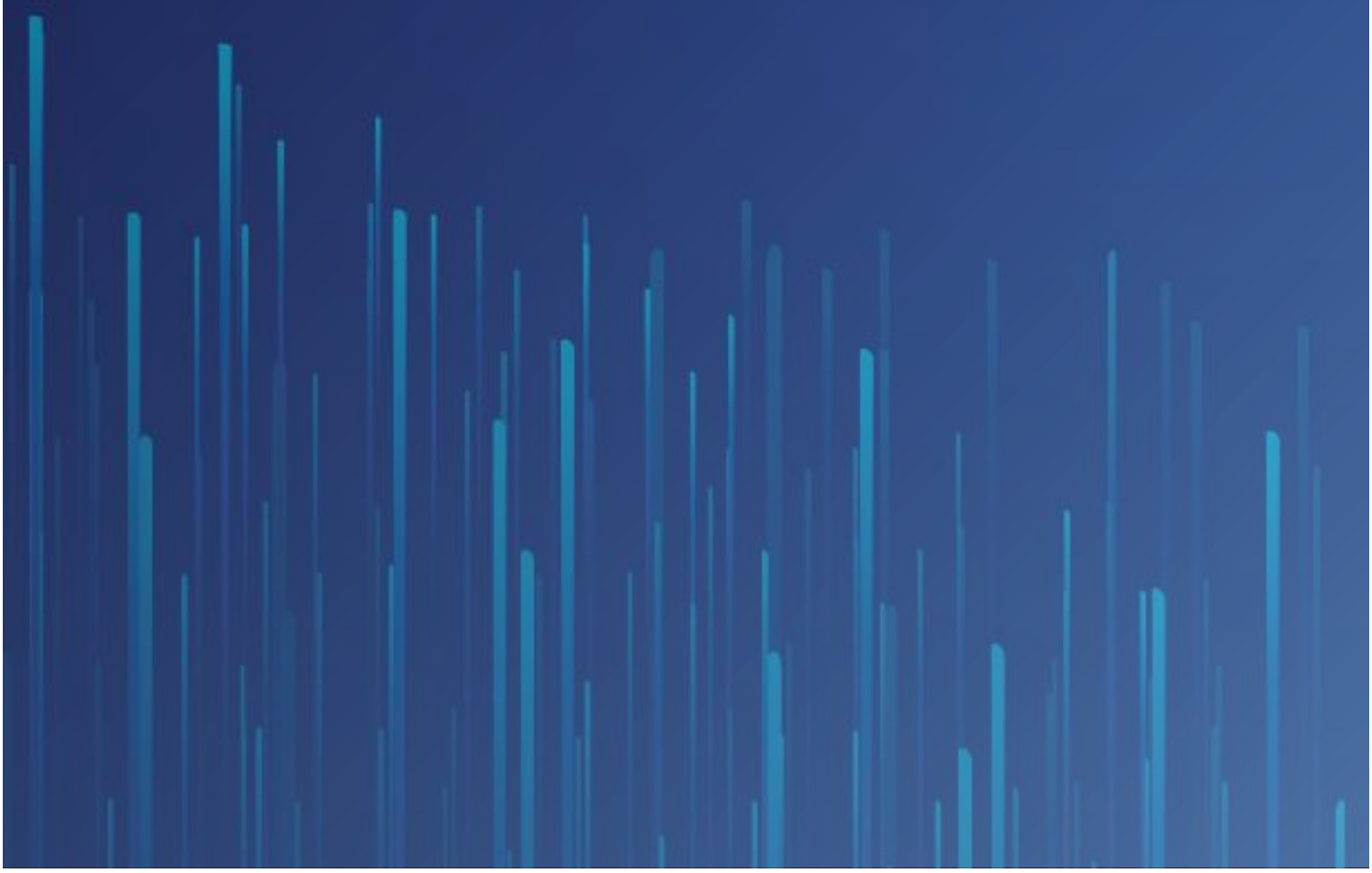
INFO~TECH
RESEARCH GROUP

Preparing Vendor Management for ESG

Best Practice Considerations

May 2023



Introduction

The importance of environmental, social, and governance (ESG) in supply chain management is a top priority for maintaining long-term corporate performance. Companies are being held accountable by regulators, consumers, and investors to consider ESG factors in their operations and to conduct business ethically and sustainably.

Today an estimated 80% of global trade passes through supply chains. Given this concentration and the potential for achieving meaningful progress toward reaching corporate ESG targets, many organizations focus their ESG efforts on third- and fourth-party suppliers.

Furthermore, ESG's tie to corporate performance leads organizations to assess ESG risks and opportunities within their supply chain by updating their assessment tools, due diligence processes, and vendor scorecards.

This report aims to provide best practice guidelines on how organizations can evaluate their current preparedness for meeting supply chain requirements and how to proactively identify, assess, and respond to supplier risk.

Environmental, social, and governance are the component pieces of a sustainability framework that is used to understand and measure how an organization impacts or is affected by society as a whole.

Example ESG issues include:

- Environment – greenhouse gas emissions, deforestation, biodiversity, pollution, water, waste, etc.
- Social – customer relations, human rights, occupational health and safety, community relations, supply chain, etc.
- Governance – Board management practices; diversity, equity, and inclusion; cyber; fraud; data hygiene; etc.

What Are Supply Chain Risks?

Climate change and greenhouse gas emissions are the most commonly discussed risks within the global supply chain. Some organizations are more carbon-intensive than others, but climate risks will somewhat affect all sectors. Understanding scope 3 emissions (indirect emissions within your value chain) and other nature-related risks can be a complex undertaking for organizations that depend on many suppliers, but how an organization manages its environmental risk is essential for building sustainable business practices.

Human rights and labor practices can present regulatory and reputational issues if left unchecked. Human rights concerns have led many regions to restrict the importation of goods from regions presumed to be using forced labor. Organizations should also actively monitor suppliers' workforce health and safety and equal pay. Reviewing the vendors' practices is a beneficial exercise in the due diligence process before engaging them in a business relationship. It is integral to ongoing monitoring once you are in a relationship.

To avoid legal action, organizations should monitor their supply chain for corruption and fraud-related activities and have auditable means to survey and assess their suppliers on their diversity, equity, and inclusion (DEI) management practices.

Legal and Compliance Obligations

Understanding legal and regulatory compliance obligations for ESG is not easy, partly because it is an evolving space, but also due to the renewed attention from lawmakers on existing mandates. For example, regulation of the supply chain comes in different forms, such as **Germany's Supply Chain Act** of January 2023 and the **Modern Slavery Act in the UK** in 2015. Regulation also comes in the form of third-party supplier guidance such as **OSFI's Third-Party Risk Management guidance (B-10) in Canada** or guidance from the **UK's Financial Conduct Authority (FCA)**, Outsourcing and Operational Resiliency. Targeted legislation is also coming from government mandates like the **US Uyghur Forced Labor Prevention Act** or direct enviormental laws like the **Clean Air Act** in the U.S.[1]

[1] The Clean Air Act is a law regulated by the United States Enviromental Protection Agency

The environmental component of ESG garners a lot of attention from regulators because of the risks climate change can pose to the economy, but the "S" and "G" components cannot be ignored. Although there is limited direct legislation on the "S" and "G" components of ESG, lawmakers are expanding requirements and embedding governance requirements into rule revisions. For example, the SEC's proposed rule, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, will require disclosure of the board's oversight of cybersecurity risks and a description of management's role in managing and assessing cyber risk.

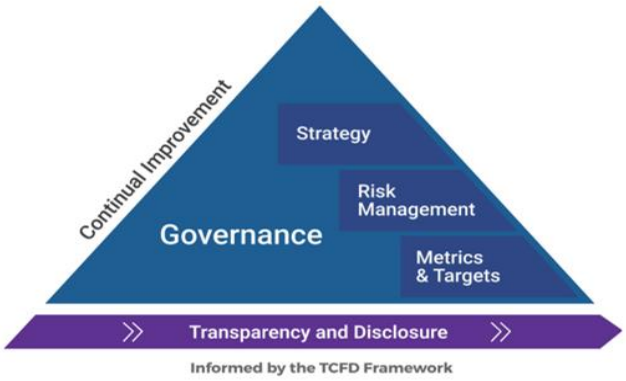
> Legislation and regulatory requirements for ESG are evolving fast; therefore, it's important that you keep abreast of your obligations. If your organization currently uses a regulatory management tool, look to extend its application to include ESG. If your organization does not use a tool, the task of understanding legal and regulatory obligations typically falls to legal and compliance. A review of regulatory changes is often a responsibility of a cross functional governance committee.

Strong Governance Is Key

Although the extent of attention needed will largely depend on the type of organization, industry, and jurisdiction in which you operate, all organizations should closely assess the negative impacts and opportunities of each ESG component by seeking legal opinion.

Part of a good governance program is to ensure you have the appropriate stakeholders involved. An effective program means ensuring compliance, legal, and audit representation in your governing council tasked with staying on top of ESG compliance and communicating changes through the organization. It is good practice to appoint a chief sustainability officer (CSO) who has a seat at the strategic level and a tactical working group with cross-functional senior leadership representation, including representation from the business, IT, audit, compliance, legal, and risk. This cross-functional working group has responsibilities such as creating and maintaining the program, assessing opportunities and risks, overseeing reporting and disclosure, and setting policies and procedures, among others. It is becoming standard practice to have procurement and third-party risk representation in the tactical working group.

Your ESG program approach should have these fundamental elements:



Integrate Risks

Supply chains are complicated and involve multiple layers. Therefore, it's important to integrate third-party risk management into your enterprise risk management program and include supply chain modeling (the method used to plan and optimize supply chain routes) to reduce risks and visualize trade-offs. The emphasis on risk management will vary across organizations, largely depending on the number of suppliers in the supply chain, internal resources, and the nature of the business. Organizations must be mindful of their supply chain's complexity to ensure that there are no hidden risks. For example, the number of corporations with foreign beneficial owners is increasing in the US, and they often obscure their ownership in shell companies and trusts. If it turns out that an ultimate beneficial owner (UBO), an owner with more than 25% of the voting rights, is on a sanctioned list, any company

> Supply chain risks should be considered against your organization's risk appetite. Any unacceptable risks, such as sourcing from certain suppliers or operating in certain geographies, should be communicated to vendor management so that assessment criteria and agreements are updated.

working with that supplier violates sanction legislation, putting them at risk of enforcement.

Prepare Your Organization

No matter the size of your organization or the resources you have at your disposal, you must have a firm grasp of your vendor landscape and the associated agreements. Understanding your vendor landscape and assessing the potential regulatory impacts and risks they might pose helps prioritize efforts and allows more time to focus on higher-risk or critical vendors.

Establish vendor standards

- Using your organization's risk appetite as a guide, determine which standards you will hold your vendors to and any new or ongoing risks you want to monitor.
- Establish metrics to measure vendors' compliance and performance.
    - Review your agreements to ensure that the vendor will be held accountable.
- Update your assessment tools, due diligence process, and vendor scorecards to reflect your expectations.
- Set a cadence for periodic review and ongoing monitoring of the vendors.
    - Ensure all the necessary parties are at the table during these reviews so that they are informed and can give feedback from their unique perspectives (Business, Compliance, Risk, Security, HR, Finance, IT, Legal, et al.).

Understand your nth-party vendor landscape

- If you are unaware of which vendors are accountable to specific regulations, you cannot effectively mitigate potential risks to your organization. Understanding who you are doing business with and what they provide your company is vital to holding them accountable to regulations.
    - Start by creating an inventory of vendors and classifying them according to their responsibilities to your organization.
        - E.g. are they strategic, tactical, operational, or commodity?
    - Make sure your assessment processes include categorizing the potential ESG risk impacts from each vendor so that you have an easy mechanism to determine which vendors are in scope for ongoing review.

For more information on vendor classification, see Jump Start Your Vendor Management Initiative | Info-Tech Research Group (infotech.com)

- Ensure that the identified vendors are mapping their nth-party support vendors and understand the relationships of those vendors.
    - You need to capture protections within the main vendor agreements from the actions of their downstream partners. If the liability remains vague, this could put your organization in a poor position later if one of the nth-party vendors is in violation.

The assessment process has multiple purposes. It helps to identify potential risks in your supply chain and creates a baseline to measure supplier performance. As your catalogue improves, it will allow you to benchmark suppliers against each other, enabling more strategic risk-based decision-making. For more information and tools to help with this assessment, see Info-Tech's blueprint **Identify and Management Regulatory and Compliance Risk Impacts on your Organization.**

Communicate with your vendor

Transparent communication and clarity about each other's expectations will enable a smooth transition to the necessary oversight and ongoing monitoring to avoid risk.

- Develop a plan of action that targets the highest-risk vendors so that you can manage your efforts to maximize value. Include some target dates in the plan to be in the best position to negotiate any changes or amendments, or include metrics in the agreement.
    - Your negotiation position is often strongest at renewal or before a major upgrade.
    - Ensure you are sufficiently aware of the procurement and IT change control processes to capture these moments before executing new agreements.
- Create a vendor orientation process to communicate changes in expectations, provide feedback, and train them on new processes.
- This communication may include a debrief, online webinar, or signed compliance statement with the new requirements.

Contractual provisions that can protect your organization

Agreements spell out the obligations and expectations that the participating organizations agree to adhere to throughout the life of their relationship. Setting the expectation that regional, governmental, and regulatory laws will apply in perpetuity –

and through their evolution – offers a great deal of protection to the non-violating partner (hopefully you).

- The assignment clause
    - Review your protections in the assignment language so a vendor acquisition does not potentially put you in a relationship with a non-compliant vendor.
        - Ex. "This Agreement and all rights and obligations hereunder may not be assigned without the written consent of the other party."
- Limits of liability
    - Ensure that the language holds the vendor accountable for all actions of subcontractors, affiliates, agents, nth-parties, and all potential actors. Unfortunately, subcontractors et al. are often only held accountable for performative actions, leaving organizations to deal directly with their violations without a formal relationship.
- Laws and regulatory obligations
    - Your agreements must clarify that the vendors – and those acting on behalf of vendors to provide you services – will abide by and be accountable to all relevant laws and regulations now and in the future. Too often, specific laws and regulations are cited, which are not revisited in the agreements when they become defunct.
    - Be sure to include language that states the vendor must not be on any non-participation or sanction list. If they violate regulations, this could automatically give you some protections without your having to engage directly.
        - Ex. "Each party will
            1. comply with all applicable Laws relating to [SUBJECT MATTER OF AGREEMENT], and
            2. notify the other party if it becomes aware of any non-compliance in connection with this section."

Summation

Navigating supply chains over the last couple of years has been difficult, and the job will not get any easier.

However, by proactively managing ESG risks within your supply chain, your organization can drive positive change and innovation while building internal resiliency against potential financial, regulatory, and reputational impacts.

Appendix

Regulatory guidance and industry standards

Organizations should leverage their legal and compliance teams to ensure they fully understand their obligations. Some of the sources to consider in your review are the following:

EU: Directive on corporate sustainability due diligence

EU: General Data Protection Regulation

EU: European Protection Agency

EU: German Supply Chain Act

Switzerland: Swiss Federal Act on Data Protection

UK: Modern Slavery Act

UK: Technology Code of Practice

UK: General Data Protection Regulation (UKGDPR)

US: Sarbanes–Oxley Act

US: Defense Federal Acquisition Regulation Supplement (DFARS)

US: Foreign Corrupt Practices Act (FCPA)

Standards and frameworks

Control Objectives for Information and Related Technologies (COBIT)

Cybersecurity Maturity Model Certification

International Organization for Standardization (ISO)

National Institute of Standards and Technology (NIST) – Third-Party Compliance Checklist

Definitions

ESG Components – Environment, social, and governance.

ESG Factors – The factors or issues that fall under the three ESG components.

Risk Appetite – An organization's general approach and attitude toward risk; the total exposed amount that an organization wishes to undertake based on risk-return trade-offs for one or more desired and expected outcomes.

Scope 3 Emissions – Scope 3 emissions pertain to emissions emitted from related parties, often referred to as third- or fourth-party suppliers, and are therefore not owned or controlled by them.

References

Contract Standards, Compliance, and Laws Covenants. www.contractstandards.com

"The Uygur Forced Labor Prevention Act." Department of Homeland Security, Dec. 2021. Accessed Mar. 2023

"Outsourcing and Operational Resilience." Financial Conduct Authority (FCA), Sept. 2020. Accessed Mar. 2023

Office of the Superintendent of Financial Institutions, "Third-party risk management guideline," Apr. 2023, Accessed Apr. 2023

"Proposed Rule: Cybersecurity Risk Management. Strategy, Governance, and Incident Disclosure." Securities and Exchange Commission (SEC), 9 Mar. 2022. Accessed Mar. 2023

Info-Tech Resources

Build an IT Risk Taxonomy

Identify and Manage Regulatory and Compliance Risk Impacts on Your Organization | Info-Tech Research Group (infotech.com)

The Assignment Clause: Why It Matters | Info-Tech Research Group (infotech.com)

The Limitation of Liability Clause – Take a Granular Approach to Identify and Manage Vendor Risk Better | Info-Tech Research Group (infotech.com)

Vendor Scorecards