Mitigating Cyber Risks in Supply Chains: A Risk-Based Approach

19. Turvallisuusjohtamisen koulutusohjelma

Lopputyöraportti

Ove Liljeqvist

Fortum Corporation

Espoo 20.3.2026

Aalto University Executive Education and Professional Development

Abstract

In today's interconnected world, supply chains are increasingly vulnerable to sophisticated cybersecurity threats that can disrupt operations and compromise sensitive information. This research report presents a risk-based model for organizations classified as essential entities under the NIS2 Directive. The model utilizes leading cybersecurity standards and frameworks, including ISO/IEC 27001 and 27002, the ISF Standard of Good Practice, and NIST's guidance for supply chain risk management. Central to the model is a tiering approach, where supplier contracts are categorized by risk, with tailored cybersecurity requirements embedded in contracts and continuous monitoring throughout the contract lifecycle. By leveraging best practices from these frameworks, organizations can systematically manage third-party risks, prioritize resources, and address regulatory obligations. Adopting this approach strengthens defenses against supply chain cyber threats, supports compliance with NIS2, and enhances business continuity and overall security posture.

Tiivistelmä

Nykyajan verkottuneessa maailmassa toimitusketjut ovat yhä alttiimpia kehittyneille kyberturvallisuusuhille, jotka voivat häiritä toimintaa ja vaarantaa arkaluonteisia tietoja. Tämä tutkimusraportti esittää riskiperusteisen mallin organisaatioille, jotka on luokiteltu NIS2-direktiivin mukaisiksi keskeisiksi toimijoiksi. Mallissa hyödynnetään keskeisiä kyberturvallisuusstandardeja ja -viitekehyksiä, mukaan lukien ISO/IEC 27001 ja 27002, ISF:n Standard of Good Practice sekä NISTin toimitusketjuriskien hallintaa koskevaa ohjeistusta. Mallin ytimessä on tiering -lähestymistapa, jossa toimittajasopimukset luokitellaan riskin perusteella, sopimuksiin sisällytetään räätälöidyt kyberturvallisuusvaatimukset, ja niiden noudattamista seurataan jatkuvasti koko sopimuksen elinkaaren ajan. Näiden viitekehysten parhaisiin käytäntöihin tukeutumalla organisaatiot voivat hallita kolmansien osapuolten riskejä järjestelmällisesti, priorisoida resursseja ja vastata sääntelyvelvoitteisiin. Tämän lähestymistavan omaksuminen vahvistaa suojautumista toimitusketjuihin kohdistuvia kyberuhkia vastaan, tukee NIS2-vaatimusten noudattamista sekä parantaa liiketoiminnan jatkuvuutta ja organisaation yleistä turvallisuuskyvykkyyttä.

Table of Contents

1 Introduction

1.1 Interconnected Environment

In today's interconnected environment, almost every organization relies on other entities. It is not economically feasible for an organization to handle everything by itself. Instead, it is more cost-effective to outsource services and products to specialized external providers. These external entities, such as subcontractors and partners, become integral parts of the organization's operations and business processes, often also handling sensitive internal information.

Further, an organization’s cybersecurity posture is inherently linked to the maturity of its supply chain. If a subcontractor suffers a cybersecurity compromise, the impact—depending on the supplier’s criticality—can result in severe consequences for the organization, including disruption of business-critical services, loss of sensitive information, reputational damage, and compliance violations. Therefore, securing only internal assets is insufficient. Effective cybersecurity risk management must explicitly extend to the entire supply chain, ensuring that third parties maintain controls at a level equivalent to the organization’s own security requirements.

1.2 Scope and Aim

This research report proposes a risk-based model for a company classified as an essential entity under the NIS2 Directive, aimed at securing its supply chain by focusing on mitigating potential cyber risks to ensure continuity and resilience. While this report discusses only EU-level legislation, organizations must also consider the relevant national implementations of NIS2 to achieve full compliance.

In order to manage supply chain risks more effectively, the aim is to classify supplier contracts into different categories, thereby prioritizing efforts and resources for cases where the risks are higher for the organization procuring a particular service or product.

In this research report, risk management activities focus on contractual and administrative tasks and arrangements for ensuring compliance. Technical measures—such as network-scanning tools—may be referenced but are not covered in detail.

Also, the focus is on cybersecurity-related risks, and other risk categories (such as financial risks) are out of scope, while it is acknowledged that the financial performance of a particular supplier could have an impact on cybersecurity as well.

2 Background

2.1 Defining Supply Chain

A supply chain is a network of individuals and companies involved in creating a product and delivering it to the consumer. This chain starts with the producers of raw materials or software components and ends when the finished product, whether physical or digital, is delivered to the user (adapted from Hayes, 2024).

Supply chain management is a crucial process because an optimized supply chain results in lower costs and a more efficient production cycle. Companies seek to improve their supply chains so they can reduce their costs and remain competitive (Hayes, 2024).

Software supply chain management is similar, but it has its own specific characteristics. For example, logistics and storage requirements are very different for software products, which can be delivered online and do not require a traditional logistics chain.

2.2 Cybersecurity in Supply Chains

Typically, organizations collaborate with numerous third-party vendors and suppliers, forming relationships that are both essential and beneficial. These partnerships aim to boost revenue, enhance customer retention, support cost control, and provide access to external resources and expertise that would not otherwise be available. In many cases, suppliers enable operations in regions where the organization lacks its own capacity or where establishing in-country capabilities would be economically impractical. With widespread digitalization, such cooperation has increased, delivering operational and financial advantages but also introducing significant cybersecurity challenges (ReliaQuest, 2024).

As cooperation has increased, it is no longer enough to protect only one's own organization. Organizations must ensure, in one way or another, that their suppliers are doing their part to implement sufficient cybersecurity measures, because cyber adversaries will exploit suppliers with weaker protections instead of directly attacking the actual target organizations, which may be better protected (Jeong, 2024).

A major reason the supply chain is targeted for cyberattacks is the weak cybersecurity measures of suppliers. Despite the increasing risk, many suppliers—often smaller companies—lack adequate protections against such attacks. With limited operational resources and capabilities, they remain vulnerable. Even when they understand the importance of cybersecurity, suppliers tend to prioritize operational performance metrics such as speed and cost over security controls (Jeong, 2024).

In addition to supplier-side weaknesses, another contributing factor is that client organizations may define insufficient cybersecurity requirements or fail to consistently enforce and monitor the controls suppliers are expected to implement. This combination of limited supplier capabilities and inadequate oversight creates systemic weaknesses that adversaries can exploit.

The SolarWinds hack, discovered in December 2020, was a significant cybersecurity breach that involved the insertion of malicious code into SolarWinds' Orion software updates. This supply chain attack affected over 18,000 organizations, including government agencies and private companies. The hackers gained access to sensitive data and networks by exploiting the privileged position of the Orion software. The breach highlighted the vulnerabilities in supply chain security and underscored the need for stronger cybersecurity measures (Oladimeji and Kerner, 2023).

The SolarWinds hack also demonstrates that suppliers are not only targeted because of weaker protections but also to gain strategic access to multiple organizations. When successful, this kind of approach increases the reach and impact of a campaign without the need to develop tools and techniques to individually breach each organization, maximizing the potential of a threat actor's resources.

2.3 Key Cyber Risk Factors within Supply Chains

According to Tuteja (2025), there are five key risk factors arising from supply chain interdependencies and contributing to an increasingly complex cyber-security landscape. These five factors are discussed in more detail below.

1. Cyber inequity: As mentioned earlier, smaller organizations often lack the resources to meet security standards, making them the weakest link in the supply chain. This inequity can compromise the entire ecosystem's resilience (Krebs, 2014).

However, inequity also exists within client organizations. Even when they have mature security practices, these capabilities may operate in silos, resulting in inconsistent application of requirements, uneven oversight, and gaps in coordination.

2. Limited visibility: As supply chains grow, it becomes increasingly difficult for organizations to maintain complete oversight of their suppliers' security practices, expanding the attack surface and elevating overall risk. This visibility gap is further exacerbated by the use of subcontractors and fourth-party vendors, where transparency is often even more limited.

Beyond simple oversight challenges, many of the methodologies used to assess supplier security—such as questionnaires or attestations—are not always sufficient for today's complex and dynamic supply-chain environments and frequently rely on trust rather than verifiable evidence.

3. Software vulnerabilities: The interconnected nature of supply chains expands the potential attack surface, making it easier for cybercriminals to exploit vulnerabilities. As supply chains expand, each new entity can introduce additional vulnerabilities, particularly when third-party compliance is difficult to verify or when open-source components are incorporated without sufficient oversight.

The rapid adoption of artificial intelligence (AI) further amplifies these challenges. Many organizations still lack mature processes to evaluate the security of AI tools before they are integrated into production environments. This gap increases the risk of unintentionally introducing weaknesses not only into individual IT estates but also across the wider ecosystem.

Compounding these issues is the persistent lack of visibility into the software itself. Limited transparency in component composition, code origin, and dependency behavior makes it harder to detect hidden risks.

4. Dependence on critical providers: Relying on a few critical providers creates systemic points of failure in supply chains. Vulnerabilities in these providers can affect their direct customers and thousands of other organizations that depend on them. Cloud providers (such as Microsoft or Amazon), or leading vendors (such as SolarWinds mentioned before), are to some extent prime examples, as their dominance means any disruption can ripple through numerous supply chains and ecosystems.

Organizations need to build resilience against these interdependency risks. Modern IT architectures composed of interconnected services make it harder to understand all dependencies and the impacts of outages.

5. Geopolitical impact on supply chains: Geopolitical factors significantly influence cyber risks, with attacks often crossing national boundaries. These tensions disrupt global supply chains by limiting access to skilled labor, essential materials, and advanced technologies, causing delays and shortages.

Additionally, geopolitical tensions escalate cybercrime, with criminals adopting advanced tools, further influencing global supply chain security. For example, Russian government-backed hackers have targeted critical infrastructure targets in Europe (Gramer, 2024).

2.4 Regulatory Environment

This section focuses on the NIS2 Directive, which is a significant part of the cybersecurity legislation in the EU. Although there are several other security-related regulations in force within the EU, such as the CER (Critical Entities Resilience) Directive, limiting examination to the NIS2 Directive is justified, particularly from the perspective of supply chain security as we see in the following chapters.

2.4.1 NIS2 Directive in General

The NIS2 Directive (European Parliament and Council, 2022) aims to strengthen cybersecurity across the EU by establishing a high common level of security for network and information systems. It builds on and replaces the original NIS Directive (European Parliament and Council, 2016) by expanding its scope and introducing more stringent requirements for risk management, incident notification, and cooperation among member states. It also addresses the evolving cybersecurity landscape and the increasing number of cyber threats.

The NIS2 Directive entered into force in January 2023, and EU Member States had until October 17, 2024, to transpose its provisions into national law (European Commission, 2025).

Key aspects of the NIS2 Directive include:

1. Expanded scope and sectoral coverage: The directive now covers a broader range of sectors and entities, including medium and large enterprises in critical sectors like energy, transport, finance, healthcare, and digital infrastructure.

2. Stricter security requirements: It introduces more stringent cybersecurity measures and obligations for companies, such as risk management, incident notification, and supply chain security.

3. Enhanced cooperation: The directive promotes better cooperation and information sharing among EU Member States to improve collective cybersecurity resilience.

4. Sanctions for non-compliance: It establishes uniform penalties across the EU for non-compliance, ensuring that organizations take their cybersecurity responsibilities seriously and face similar consequences regardless of their location. Administrative penalties can be up to 10 MEUR or 2 % of the world-wide annual turnover, whichever is higher.

5. Management accountability: The directive places greater responsibility on the top management of organizations to ensure compliance with cybersecurity requirements.

2.4.2 NIS2 and the Supply Chain

For companies within the scope of NIS2, one of the directive's most impactful provisions is its emphasis on managing cybersecurity risks within the supply chain. By mandating stricter oversight of third-party relationships and requiring organizations to assess and mitigate risks posed by external service providers, NIS2 aims to close a major vulnerability that has been exploited in numerous high-profile cyberattacks.

Article 21 requires entities to implement appropriate technical, operational, and organizational cybersecurity measures, following an all-hazards approach. These measures shall address supply chain security, including the security aspects of relationships with direct suppliers and service providers. Entities must consider the specific vulnerabilities of each supplier and the overall quality of their products and cybersecurity practices, including secure development procedures (ENISA, 2023).

According to Finnish Transport and Communications Agency (Traficom, 2025), this risk-based approach to managing cybersecurity risks associated with third-party suppliers and service providers includes:

1. Security requirements in contracts: Entities shall ensure that cybersecurity requirements are addressed in supplier relationships. Where appropriate, these requirements should be defined in contracts, covering matters such as incident reporting, data protection, and the implementation of proportionate technical and organizational security measures. Entities may also require suppliers to adhere to relevant security standards (e.g., ISO/IEC 27001) where justified by risk.

2. Oversight and auditing: Entities shall integrate suppliers into their cybersecurity risk management process. Depending on the supplier's criticality and risk profile, entities should apply proportionate oversight measures, which may include periodic assessments, reviews, or audits to verify that agreed cybersecurity requirements are met.

3. Supply chain mapping and analysis: Entities should maintain an up-to-date list of their direct suppliers and service providers, including identification of critical suppliers and key dependencies.

4. Incident and vulnerability disclosure: Suppliers should be required to promptly disclose any cybersecurity incidents or vulnerabilities that may impact the organization. There should be clear communication channels and escalation procedures in place.

5. Third-party risk management policies: Organizations should establish formal policies and procedures for managing third-party risks. This includes onboarding, ongoing evaluation (i.e. monitoring), and offboarding processes with cybersecurity considerations.

2.5 Cybersecurity Standards and Frameworks

In this section, we analyze a couple of widely adopted cybersecurity standards and frameworks. Rather than covering these standards in their entirety, we concentrate on the elements most relevant to managing cybersecurity risks within the supply chain context.

2.5.1 ISO 27000 Series

ISO/IEC 27001 is an internationally recognized standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

It provides a systematic approach to managing an organization's sensitive information, ensuring its confidentiality, integrity, and availability. The ISMS should be integrated with the organization's processes and overall management structure, and information security should be considered in the design of processes, information systems, and controls. The standard is applicable to organizations of all sizes and sectors, and it supports risk-based thinking to address evolving security threats (ISO/IEC, 2022a).

ISO/IEC 27002 complements ISO/IEC 27001 by offering detailed guidance on the implementation of the controls listed in Annex A of ISO/IEC 27001. While ISO/IEC 27001 outlines what needs to be done, ISO/IEC 27002 explains how to do it. It includes a framework of best practices and practical recommendations for implementing controls related to areas such as access control, incident management, physical security, and supplier relationships (ISO/IEC, 2022b).

In the context of supply chain security, both standards provide essential recommendations. While ISO/IEC 27001 includes specific controls under Annex A that address the management of supplier relationships and the protection of organizational assets, ISO/IEC 27002 expands on these controls by advising concrete actions such as conducting supplier risk assessments, establishing clear cybersecurity clauses in contracts, and regularly reviewing supplier compliance.

There are seven control areas in ISO/IEC 27002 that are primarily focused on supply chain security. These areas can be found under “Organizational”, “People” and “Technological” controls and are listed in Table 1.

Table 1 Supply chain related security controls in ISO/IEC 27002:2022

Control	Title	Description
5.19	Information security in supplier relationships	Focuses on managing risks by implementing tailored policies, vetting suppliers, and ensuring ongoing compliance, aiming to protect organizational data throughout the entire supplier lifecycle
5.20	Addressing information security within supplier agreements	Control emphasizes clear and mutually agreed-upon cybersecurity obligations. It ensures that both parties understand and commit to protecting sensitive data through defined access

		controls, compliance measures, and risk mitigation strategies
5.21	Managing information security in the ICT supply chain	Control requires organizations to establish and enforce agreed security standards for suppliers, ensuring that providers, including those offering cloud services, maintain consistent practices throughout the supply chain
5.22	Monitoring, review and change management of supplier services	Focuses on monitoring, reviewing, and managing changes in supplier services to ensure they continue to meet agreed security and service standards. It helps organizations to stay in control of risks that could affect operations
5.23	Information security for use of cloud services	Control ensures that organizations manage risks by clearly defining responsibilities, setting security expectations, and maintaining oversight throughout the cloud service lifecycle. Promotes a shared responsibility model between the organization and the cloud provider
6.6	Confidentiality or non-disclosure agreements	Non-disclosure agreements (NDAs) protect sen-

		sitive information from being leaked or misused. Control ensures that anyone with access to confidential data - whether employees, partners, or third parties - understands and agrees to their responsibilities for keeping information secure
8.30	Outsourced development	Aims to ensure that when software development is outsourced, providers follow the organization's security requirements. Supervising and monitoring third-party development are key to protecting the confidentiality, integrity, and availability of systems and data

2.5.2 National Institute of Standards and Technology (NIST)

NIST is a non-regulatory agency of the United States Department of Commerce. NIST's primary functions include developing technology, metrics, and standards that are essential for innovation and industrial competitiveness.

NIST has published a comprehensive framework for managing cybersecurity risks throughout the supply chain (NIST, 2022). This publication, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations" addresses the growing complexity and interdependence of modern supply chains, emphasizing the need for organizations to identify, assess, and mitigate risks associated with third-party products and services.

The framework aligns with broader U.S. federal government cybersecurity initiatives and integrates with other risk management frameworks, such as the

NIST Cybersecurity Framework (CSF). It is designed to be flexible and scalable, making it suitable for organizations of all sizes and sectors. This adaptability allows organizations to implement effective supply chain risk management strategies tailored to their specific needs and circumstances.

According to NIST (2022), the following key controls and practices should be implemented to enhance the efficacy of cybersecurity supply chain risk management:

1. Establish a Cybersecurity Supply Chain Risk Management (C-SCRM) strategy and governance program: Develop a C-SCRM strategy aligned with organizational risk tolerance and mission, and assign roles and responsibilities across the organization. Obtain senior leadership's support for the work.

2. Integrate C-SCRM into the life cycle processes: Apply C-SCRM practices throughout the acquisition, development, deployment, and maintenance of systems. Include security requirements in contracts and procurement documents. Conduct supplier due diligence and risk assessments during vendor selection. Identify critical suppliers.

3. Assess and monitor suppliers and supply chain risks: Continuously assess suppliers for cybersecurity posture, compliance, and risk exposure. Use third-party risk management tools (including vulnerability scanning) and threat intelligence to monitor supply chain threats. Utilize third-party assessment surveys, on-site visits, and formal certifications (e.g. ISO 27001) to assess supplier security capabilities and practices. Also, require suppliers to provide Software Bills of Materials (SBOMs) and security attestations.

4. Implement an incident management program: The program should be able to successfully identify, respond to, and mitigate security incidents, including those that originate from the supply chain. Also, make sure that suppliers and service providers actively identify and disclose vulnerabilities in their products.

5. Report and train: Define, collect, and report C-SCRM metrics to ensure risk-aware leadership, enabling active management of the C-SCRM implementations, and driving the effectiveness of the organization's C-SCRM pro-

cesses and practices. Coordinate with the organization's cybersecurity program leadership to escalate top C-SCRM risks to the senior management or risk committee.

Incorporate C-SCRM-specific training into the training programs of applicable roles across the organization involved with C-SCRM, including information security, procurement, risk management, engineering, software development, IT, legal, and HR.

2.5.3 ISF Standard of Good Practice

The Information Security Forum (ISF), founded in 1989, is an international organization aimed at enhancing the information security of its member organizations. It is an independent, non-profit organization whose membership consists of large corporations and public sector organizations from around the world (ISF, 2025).

ISF members have access to a wide range of research, integrated tools, and methodologies, including a security framework called the ISF Standard of Good Practice (SOGP). The SOGP framework is a globally recognized, implementation-level standard that provides practical guidance on managing cybersecurity risks. It is designed to help organizations respond to evolving threats, align with international standards, and integrate security into business operations (ISF, 2024).

The SOGP encompasses a comprehensive range of security domains, including governance, risk management, endpoint protection, system development, and industrial control systems. Notably, for the purposes of this research report, the SOGP provides dedicated guidance on supply chain security and the secure acquisition and management of cloud services.

It outlines a structured approach to implementing a supplier security management framework, ensuring that security requirements are embedded throughout the procurement lifecycle. This includes defining and applying appropriate security controls when sourcing products and services from external suppliers, and integrating these requirements into contractual agreements.

Furthermore, the SOGP emphasizes the importance of ongoing oversight by recommending continuous monitoring and assessment of external suppliers' security arrangements. This ensures that suppliers remain compliant with agreed-upon controls and that any emerging risks are promptly addressed. Table 2 lists all supply chain-related controls mentioned in the SOGP.

Table 2 Supply chain-related security controls in the ISF Standard of Good Pratice (SOGP)

Control	Title	Description
SC1.1	Supplier Management Framework	A documented supplier management framework should be implemented, incorporating external supplier security steering groups, relevant policies, procedures, registers, information risk assessments, and appropriate security measures.
SC1.2	Supplier Procurement	A process for supplier procurement should be established to ensure security requirements are defined, suppliers are assessed for their ability to meet these requirements, and the information security function is involved in evaluating and selecting only those suppliers that adequately address information security risks.
SC1.3	Supplier Contracts	The use of products and services provided by external suppliers should be supported by contracts that include appropriate security requirements. For example, contracts should require suppliers to protect information, ensure compliance with regulatory standards,

		support audits and incident response, notify of changes, and enable secure contract exit. All contracts must be reviewed, approved, and regularly updated.
SC1.4	Supplier Assurance	The security arrangements of suppliers should be continuously monitored and assessed, using a mix of methods such as supplier self-assessments, certifications, on-site audits and external security ratings. The goal is to ensure suppliers meet agreed security requirements, comply with legal and contractual obligations, and address any weaknesses promptly. Results should be reported to stakeholders, with recommendations for remediation or contract changes if needed, helping to keep supplier-related risks within acceptable limits.
CS1.1	Cloud Security Management	A comprehensive approach for the secure acquisition, development, and use of cloud services should be developed and communicated. This includes establishing a cloud security governance framework, evaluating the security implications of different cloud deployment types and service models, and maintaining a register of cloud services in use. Roles and

		responsibilities for cloud security should be clearly defined. This control emphasizes the implementation of core cloud security controls—such as network security, access management, secure configuration, and security monitoring—by trained practitioners. The control also recommends evaluating cloud security products and services, including how they integrate with each other and with existing technical infrastructure and security solutions.
CS1.2	Core Cloud Security Controls	A set of fundamental cloud security controls should be created and tailored to the organization's needs. These controls include securing network connections to cloud services, robust access management, the use of multi-factor authentication, and protecting data with encryption and data leakage prevention. They also require secure configuration of cloud resources (such as standard builds and secure APIs) and continuous security monitoring, including vulnerability management and integration with incident management processes.

3 Risk-Based Model for Cybersecurity in Supply Chains

3.1 Framework Overview

In the previous section, we introduced various cybersecurity standards and frameworks. Our risk-based model will build on these by drawing on common best practices. In particular, we focus on identifying critical suppliers and establishing a categorization method for supplier contracts to ensure that organizational resources are allocated efficiently. It is important to note that in practice, supplier contracts are assessed individually, as an organization may maintain several contracts with the same supplier, each carrying a different level of risk.

3.2 Categorizing Suppliers Based on Risk

The NIS2 Directive requires organizations to assess and manage supply chain cybersecurity risks, including understanding the security practices of their direct suppliers. In practice, this typically necessitates maintaining an up-to-date view of suppliers, for example through a contract database. Without a complete picture of suppliers, it would be nearly impossible to manage the risks they pose to an organization.

When procuring a new service or product, the first step is to assess the potential risks a supplier may pose to business operations, such as service outages or data breaches involving the organization’s data or connections to its production environment.

3.2.1 Business Impact Analysis

In assessing these risks, a Business Impact Analysis (BIA) is a valuable tool to systematically analyze all potential outcomes, preferably in monetary terms to ensure comparability between different assessments. BIA is a pro-

cess that predicts the potential consequences of a disruption to critical business functions. It helps organizations identify operational and financial impacts, prioritize critical processes, and plan for resilience against disruptions such as supply chain failures, IT outages, or natural disasters (FEMA, 2023).

Building on this, conducting a BIA in a procurement context focuses on the specific service or change under review rather than the entire organization. The analysis begins by identifying the critical activities within the defined scope and examining the people, technology, data, and third-party services they rely on. Mapping these dependencies highlights where vulnerabilities or single points of failure may exist and clarifies which resources are essential for continuity (MetricStream, 2025).

Once the critical activities and dependencies are understood, the potential effects of downtime are evaluated by determining how long each function can be interrupted before the impact becomes unacceptable. This leads to defining acceptable recovery timeframes, such as the Recovery Time Objective (RTO), which indicates how quickly an activity must resume to prevent significant harm. These insights support the prioritization of recovery actions so that functions with the highest impact or shortest tolerances receive attention first. The results are then integrated into continuity and recovery planning to ensure that decisions and mitigation measures reflect the operational realities of the specific service being assessed. A simplified example is illustrated in Figure 1 (MetricStream, 2025).

Business Impact Analysis (BIA)

Critical Business Process / Service	Dependency	Recovery Time	Reputational Impact	Financial Impact
Payroll	HR system	8 hours	High	> 200 000 eur

Figure 1 An example of Business Impact Analysis (adapted from FEMA, 2023)

When performing a BIA in this context, it's essential to evaluate the supplier's contribution to delivering a specific service in relation to the organization's own role. For example, in a Software-as-a-Service (SaaS) model, the supplier plays a dominant role—possibly creating a higher level of risk for the organization—whereas in some critical business services, the supplier's involvement may be minimal, resulting in lower associated risk.

Although a BIA and a risk assessment are closely related, they serve distinct but complementary purposes. The BIA focuses on the effects of disruptions on critical operations and helps prioritize recovery efforts, whereas a risk assessment identifies potential threats and evaluates the likelihood that they will occur. In practice, the risk assessment highlights the "what if", and the BIA answers the "so what". For instance, while a risk assessment may identify the possibility of a data breach, the BIA quantifies its impact on customer trust, legal compliance, and operational efficiency—providing the necessary context to understand the true severity of the supplier-related risk.

3.2.2 Tiering Model

Once a BIA has been completed and a supplier's role in the overall service is clear, we can begin the classification process by using the following examples for possible outcomes to evaluate a disruption or deviation related to service delivery:

1. Severe operational disruption for the organization's business
2. Considerable harm to the organization's customers or society
3. Considerable financial loss for the organization

In the context of an energy sector organization, a severe operational disruption may involve the shutdown of a major power plant or critical site, resulting in halted or suboptimal power generation and consequent revenue losses. The precise definition of "severe" should be established separately and aligned with the organization's overall operational framework. For example, a business area owning the production in question might set a threshold, such as disruptions lasting over four hours, to classify an incident as severe.

Similarly, significant harm to customers or society may occur when a substantial portion of customers are unable to access essential services such as electricity or heating. In the case of a data breach, this could involve the compromise of personal information, leading to identity theft and fraudulent activities carried out in the customers' names. In addition, potential environmental consequences should be considered, particularly in situations where operational failures could endanger critical infrastructure such as dam safety.

Finally, "considerable financial loss for the organization" can be understood as a situation in which other possible disruptions or deviations are assigned a

monetary threshold that is considered unacceptable, thereby requiring mitigating actions, especially when a supplier may be a cause of the loss. Again, each business area needs to define its risk appetite by setting a monetary threshold for acceptable loss. While this risk overlaps with the two previous risk types, it emphasizes the evaluation of potential impacts in financial terms.

If the initial analysis indicates that a supplier (contract) is a potential source of any of these three risks, a subsequent analysis is conducted using the following illustrative questions:

4. A significant amount of personal data or other sensitive information is at risk of loss or leakage (i.e. a possibility for a major financial or reputational impact)?
5. The supplier contract involves technical integrations that could impact critical operations (e.g., energy production)?
6. Capability to run essential internal IT processes is endangered (e.g., authentication to most of the systems)?

As before, the business must set clear limits. For instance, endangering data belonging to more than 50,000 people could be considered significant in this context. Similarly, thresholds for outages and loss of production for the latter questions must be set to reduce ambiguity and ensure relevance for the business in question.

If the subsequent analysis indicates that any of these three scenarios is likely to occur, the supplier contract is classified as critical (Tier 1). This designation reflects a high level of risk and warrants the allocation of greater internal resources relative to the other tiers. Conversely, if these scenarios are deemed unlikely, the contract is categorized as important (Tier 2), representing a medium level of risk for the organization.

The classification process concludes by evaluating outcomes where the initial analysis reveals a very low probability for those outlined risks. In such cases, a further assessment is carried out to determine the presence of:

7. A limited amount of personal data or other confidential information
8. Technical integrations to non-critical systems

For clarity, “a limited amount of personal data” may be defined as information related to no more than 5,000 individuals, comprising basic details such as names, addresses, or phone numbers and excluding sensitive identifiers like social security numbers. Similarly, any technical integration by the supplier pertains exclusively to non-critical systems. Ultimately, this analysis is intended to ascertain whether the supplier contract presents a low likelihood of significant impact on the organization.

If either condition is met, the supplier contract is classified as a standard (Tier 3). When neither criterion applies, and the contract scope contains no digital component that could affect the confidentiality, integrity, or availability of business operations or data—for example, a logistics service for spare parts—it is considered a “contract without cybersecurity relevance,” as cybersecurity is not a material factor in its execution.

The complete process is depicted in Figure 2.

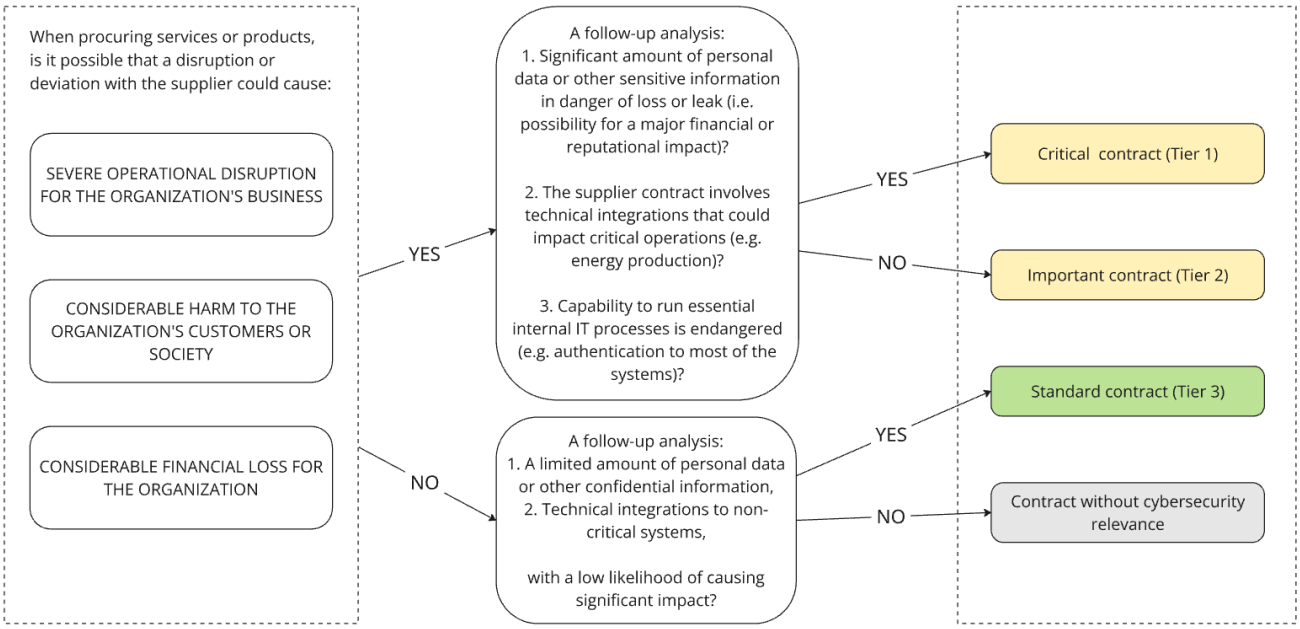

Figure 2 Supplier contract classification process

3.3 Establishing Contractual Requirements

All the standards and frameworks discussed in the previous section emphasized the importance of contracts concluded with suppliers, in which

the cybersecurity requirements must be clearly documented. For example, the ISF SOGP recommends that contracts should require suppliers to protect information, ensure compliance with regulatory standards, support audits and incident response, notify of changes, and enable secure contract exit, among other things. In addition, all contracts must be reviewed, approved, and regularly updated.

In this chapter, we will not examine individual requirements or the detailed content of contracts. Instead, we present an example model of how the previously introduced risk-based supplier contract classification (tiering model) could influence contracts and their negotiation process.

The first step is to establish a standard set of cybersecurity requirements that serves as the baseline for all contracts. ISO/IEC 27002 is a strong foundation for this, as it is widely recognized and understood by suppliers. This baseline can be applied directly to low-risk or "standard" contracts (Tier 3), where only minimal cybersecurity expertise is needed and the procurement function can manage supplier assessments and negotiations largely on its own.

One practical approach is to use a self-assessment questionnaire based on the baseline requirements, which all suppliers participating in the tender process must complete. The questionnaire supports the contractual requirements, and areas deemed out of scope can be mutually agreed upon, since not all security controls are relevant in every situation (for example, secure development requirements are not applicable if software development is out of scope).

For contracts assessed as critical or higher risk (Tier 1 or Tier 2), procurement should involve cybersecurity specialists. Additional, case-specific security requirements should be defined to address risks that the baseline alone does not sufficiently cover. Baseline requirements may also need to be modified. Cybersecurity experts can also conduct a more detailed evaluation of the supplier's security posture, review audit or assurance reports, and request further evidence of implemented controls where necessary.

The distinction between Tier 1 and Tier 2 at this stage typically relates to the level of scrutiny and the acceptable risk threshold. Tier 1 contracts generally require more rigorous examination of the supplier's security processes and controls, along with a lower tolerance for residual risk compared with Tier 2 engagements.

There are naturally situations where our negotiating leverage is limited, particularly with large providers such as Amazon or Microsoft. In these cases, we may not have audit rights and must remain flexible with certain other requirements as well. As a result, greater reliance is placed on independent audit reports, which these types of providers typically make publicly available.

On the positive side, established global providers usually have mature security processes and significant resources, and in many areas they maintain more stringent controls than what we could reasonably require from smaller suppliers—or what would be feasible from a business-case perspective.

3.4 Continuous Monitoring and Assessment

At this stage, the contract has been signed with the selected supplier, and the product or service has been taken into use. The security controls selected through the risk assessment process have also been implemented.

The next step is to establish a monitoring plan based on the supplier contract. This ensures that the supplier continues to meet the agreed security requirements, complies with all legal and contractual obligations, and promptly addresses any weaknesses or incidents. Effective monitoring helps to keep supplier-related risks within acceptable levels by reducing the likelihood of supply chain breaches, regulatory penalties, and reputational damage.

Earlier, when discussing cybersecurity standards and frameworks, we noted that the ISF SOGP recommends continuous monitoring and assessment of supplier security arrangements through a combination of methods such as supplier certifications, on-site audits, and external security ratings. Similarly, NIST highlights the use of third-party risk management tools—including vulnerability scanning—and threat intelligence to track supply chain threats. NIST also advises using on-site reviews, and formal certifications (e.g., ISO/IEC 27001) to evaluate supplier security capabilities and practices in this phase of a contract lifecycle.

Depending on the contract terms, if the supplier is required to maintain a specific security certification, it should be confirmed that the certification remains valid. Likewise, if the supplier has committed to providing an independent assurance report—such as a SOC 2 Type II report (Shvueli, 2025)—it is important to confirm that the report is available and up to date. This becomes

particularly critical when the contract does not grant us the right to conduct our own audit.

3.4.1 Applying Tiering Model

How does this apply to our tiering model? For Tier 3 contracts, no continuous monitoring is performed. Instead, actions are taken only in response to specific incidents or issues as they arise. This approach helps conserve resources for higher-risk contracts. In contrast, Tier 1 and Tier 2 supplier contracts require proactive monitoring and regular assessments to manage their higher risk levels effectively. In addition to verifying that the supplier operates according to the agreement, it is essential to regularly confirm that requirements and contact information are current, and that security practices—including incident management processes—continue to meet our needs.

As implied above, audit and assurance reports are valuable sources of information for ensuring supplier risks remain within acceptable levels. Past experience with the same supplier in other engagements can also provide useful insights for risk estimation. In practice, it is recommended to integrate this security dialogue into regular service management meetings (or similar forums) with the supplier, rather than treating it as a separate exercise. These discussions should cover a range of relevant topics—such as past incidents and their resolution, cybersecurity-related changes, compliance status, audit findings, and opportunities to maintain or improve the security posture. For Tier 1 contracts, continuous monitoring should occur annually, while medium risk Tier 2 contracts can be reviewed less often, such as every two years. Table 3 summarizes the monitoring approach and frequency by tier.

Table 3 Tier-based monitoring

Tier	Risk Level	Monitoring Approach	Frequency
1	High	Regular assessments	Annual
2	Medium	Regular assessments	Every two years
3	Low	Reactive only	As needed

3.5 Implementation Notes

3.5.1 Governance and Risk Ownership

The proposed model is best operated through sustained cooperation between Procurement, Business Owners, Service Management, and Cybersecurity, with Legal and Privacy consulted when needed. Responsibilities should be defined by roles rather than named individuals so that continuity is preserved through reorganizations, and role-based ownership is maintained across sourcing, contracting, operation, change, and exit to prevent handoff gaps, as no single unit owns the full lifecycle.

The contract's risk level is kept as low as reasonably possible, taking business needs, costs, and available vendors into account. Any remaining residual risks are accepted only by authorized roles, documented with rationale and compensating controls, and revisited when circumstances change. If it appears that an excessive level of cyber-related risk is being accepted by the business owning the contract, the decision is to be challenged and, if necessary, escalated through the appropriate channels.

3.5.2 Tier Lifecycle and Cost Justification

As Tier values are directly tied to risks, tier outcomes may also be adjusted where justified. A contract initially classified as Tier 2 may be downgraded to Tier 3 when credible, tested continuity arrangements materially reduce impact, while an initially Tier 3 contract may be upgraded to Tier 2 when hidden integrations to critical data are revealed. Re-classification is also needed when the contract's scope or integrations change, when the nature or volume of data shifts, after incidents, after material supplier changes, or on a scheduled cadence to prevent drift.

While contract classification is intended to support efficient resource allocation, higher-risk tiers still require assessment and monitoring capacity, and associated costs are incurred. Given the ongoing nature of this workload, a clear business case is required: compliance with regulation is one aspect, but it must also be demonstrated that the cost is recovered through avoided losses, as the likelihood of severe risks materializing—and the resulting high-impact incidents—is reduced.

4 Conclusions

This research report has demonstrated that effective cybersecurity in supply chains is fundamentally a matter of risk management—balancing the allocation of resources against the likelihood and potential impact of cyber threats. The risk-based model presented here, grounded in leading standards and frameworks (ISO/IEC 27001/27002, NIST, ISF SOGP), provides a systematic approach for organizations to identify, assess, and mitigate third-party risks in line with regulatory requirements such as the NIS2 Directive.

A key insight is that “good enough” security is context-dependent: organizations must define acceptable risk levels and tailor their controls accordingly. While regulations like NIS2 provide a baseline and can make compliance more straightforward, the ultimate responsibility for business continuity and resilience remains with the organization itself. Investments in supply chain cybersecurity—whether direct (e.g., external audits) or indirect (e.g., staff time spent on monitoring-related activities)—may be difficult to justify in terms of return on investment, especially when successful risk management means that nothing adverse happens. Nevertheless, the cost of inaction or insufficient controls can be far greater, as demonstrated by high-profile supply chain breaches.

Trust, but verify, is a guiding principle. Contracts alone are insufficient if not actively enforced and followed up. Continuous monitoring, regular assessments, and clear communication channels with suppliers are essential to ensure that agreed-upon security requirements are maintained throughout the contract lifecycle. This is particularly important for critical supplier contracts (Tier 1), where the risk and potential impact are highest.

Implementation challenges remain, particularly in securing business buy-in for the financial and operational costs associated with ongoing monitoring. It is crucial to clearly communicate the risk-reducing value of these activities,

not only for regulatory compliance but for the organization's own long-term interests.

Future work could deepen the model by integrating more granular BIA and risk assessment methods and by defining Key Performance Indicators (KPIs) that objectively measure assessment throughput, remediation timeliness, and residual-risk trends. A further extension would be to compare country-level implementations and national legislation to understand how local regulatory differences shape supplier requirements, oversight practices, and cross-border sourcing decisions.

In summary, a risk-based approach enables organizations to prioritize their efforts, allocate resources efficiently, and build resilience against evolving supply chain cyber threats. By embedding security requirements in contracts, maintaining robust oversight, and fostering a culture of continuous improvement, organizations can better safeguard their operations, reputation, and compliance posture in an increasingly interconnected world.

5 References

ENISA (European Union Agency for Cybersecurity). 2023. Good Practices for Supply Chain Cybersecurity. [online] Available at: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity [Accessed 30.04.2025].

European Commission. 2025. NIS2 Directive: new rules on cybersecurity of network and information systems. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive [Accessed 24.04.2025].

European Parliament and Council. 2016. Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. [online] Available at: https://eur-lex.europa.eu/eli/dir/2016/1148 [Accessed 24.04.2025].

European Parliament and Council. 2022. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). [online] Available at: https://eur-lex.europa.eu/eli/dir/2022/2555 [Accessed 24.04.2025].

Federal Emergency Management Agency (FEMA). 2023. Business Impact Analysis. [online] Available at: https://www.ready.gov/business/planning/impact-analysis [Accessed 25.09.2025].

Gramer, R. 2024. Russia Ramps Up Sabotage Operations in Europe. Foreign Policy. [online] Available at: https://foreignpolicy.com/2024/06/13/russia-sabotage-attacks-europe-espionage-hybrid-arson/ [Accessed 20.03.2025].

Hayes, A. 2024. The Supply Chain: From Raw Materials to Order Fulfillment. Investopedia. [online] Available at: https://www.investopedia.com/terms/s/supplychain.asp [Accessed 23.12.2024].

ISF (Information Security Forum). 2024. The ISF Standard of Good Practice for Information Security 2024. [online, restricted access] Available at: https://www.isflive.org/s/isf-assure/standard-of-good-practice [Accessed 04.08.2025].

ISF (Information Security Forum). 2025. A Leading Authority on Information Security and Risk Management. [online] Available at: https://www.securityforum.org/about-us/ [Accessed 04.08.2025].

ISO/IEC. 2022a. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. [online] Available at: https://www.iso.org/standard/27001 [Accessed 14.05.2025].

ISO/IEC. 2022b. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. [online] Available at: https://www.iso.org/standard/75652.html [Accessed 14.05.2025].

Jeong, S. 2024. Cybersecurity as a major supply chain risk domain. Supply Chain Management Review. [online] Available at: https://www.scmr.com/article/cybersecurity-as-a-major-supply-chain-risk-domain [Accessed 23.01.2025].

Krebs, B. 2014. Target Hackers Broke in Via HVAC Company. KrebsOnSecurity. [online] Available at: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ [Accessed 26.01.2026].

MetricStream. 2025. Business Impact Analysis: Why, When, and How to Do It Effectively. [online] Available at: https://www.metricstream.com/learn/business-impact-analysis.html [Accessed 12.03.2026].

National Institute of Standards and Technology (NIST). 2022. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST Special Publication 800-161 Revision 1, updated 2024. [online]

Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf [Accessed 02.06.2025].

Oladimeji, S. and Kerner, S. 2023. SolarWinds hack explained: Everything you need to know. TechTarget. [online] Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [Accessed 10.02.2025].

ReliaQuest. 2024. Threat Spotlight Report: Beyond Your Borders: Managing Third-Party Risk. [online] Available at: https://www.reliaquest.com/blog/managing-third-party-risk/ [Accessed 31.12.2024].

Shvueli, R. 2025. Understanding SOC 2 Type 2 Audits & 5 Tips for Passing Yours. Venn. [online] Available at: https://www.venn.com/learn/soc2-compliance/soc-2-type-2/ [Accessed 05.01.2026].

Traficom (Finnish Transport and Communications Agency). 2025. Recommendation on cybersecurity risk management measures for NIS supervisory authorities. [online] Available at: https://www.kyberturvallisuuskeskus.fi/en/regulations/recommendation-nis-supervisory-authorities-cybersecurity-risk-management-measures [Accessed 06.05.2025].

Tuteja, A. 2025. Five risk factors from supply chain interdependencies in a complex cybersecurity landscape. World Economic Forum. [online] Available at: https://www.weforum.org/stories/2025/01/5-risk-factors-supply-chain-interdependencies-cybersecurity/ [Accessed 11.02.2025].