Supply Chain Risk Assessment

Dhia Gabtni

February 10, 2025

—

EUS Cloud GmbH

—

NIS 2

Network and Information Systems Directive 2

Directive (EU) 2022/2555

Abstract

This document presents a **NIS 2** compliance gap analysis for **EUS Cloud GmbH**, a fictional mid-sized company based in Spain. The objective of this project is to simulate a realistic consulting engagement to identify gaps in **NIS 2** compliance and recommend actionable solutions. By conducting this analysis, the author aims to deepen their understanding of cybersecurity consulting practices and regulatory frameworks, specifically focusing on **NIS 2**.
The report follows a structured approach, starting with an overview of the fictional organization and its data handling practices, progressing to the identification of compliance gaps, and concluding with practical recommendations. This exercise is designed as a hands-on learning project to showcase key skills in compliance assessment, risk management, and strategic recommendations for regulatory alignment.

As a personal project, this analysis reflects hypothetical scenarios and assumed practices, making it an educational exploration of the challenges and opportunities within the cybersecurity consulting space.

Table of Contents

Tables

Table of Figures

Executive Summary

1. Purpose of the Report

This report presents a comprehensive supply chain cybersecurity risk assessment for **EUS Cloud GmbH**, aligned with the latest requirements of the NIS 2 Directive. The assessment focuses on identifying risks associated with third-party vendors and evaluating the organization's readiness to meet **NIS 2** compliance standards.

2. Key Findings

Key findings from the assessment revealed significant vulnerabilities, including insufficient security controls among critical vendors, lack of standardized vendor risk assessments, and gaps in incident reporting processes. These issues pose potential risks to regulatory compliance, data security, and operational continuity.

3. Key Recommendations

To address these gaps, this report recommends the following priority actions:

- Implement a formalized vendor risk management framework to evaluate and monitor third-party compliance.
- Develop an incident reporting process to meet NIS 2 requirements, including a 24-hour notification procedure and 30-day root cause analysis reports.
- Strengthen contractual agreements with vendors to include specific cybersecurity obligations like regular security audits.

4. Value of Compliance

By addressing these vulnerabilities, **EUS Cloud GmbH** can enhance its supply chain security, reduce regulatory risks, and align its operations with the harmonized cybersecurity framework established by the **NIS 2 Directive**.

Introduction

1. Background and Context

The **NIS 2 Directive**, adopted by the European Union in 2022, establishes stringent cybersecurity requirements for critical sectors and essential entities, including cloud service providers. A key focus of the directive is securing supply chains to prevent vulnerabilities introduced by third-party vendors. For cloud service providers, which rely heavily on external vendors for infrastructure, software, and operational support, supply chain security is paramount to ensuring regulatory compliance and operational resilience.

2. Purpose

This report aims to assess the supply chain cybersecurity risks of **EUS Cloud GmbH** and evaluate its readiness to meet the requirements of the **NIS 2 Directive**. The assessment focuses on identifying vulnerabilities in third-party vendor relationships, analyzing compliance gaps, and providing actionable recommendations for improvement.

3. Scope of the Assessment

The scope of this report includes:

- Evaluating the cybersecurity practices of key third-party vendors.
- Identifying non-compliant or high-risk vendors and their impact on overall security.
- Assessing the organization's risk management and incident response practices in relation to supply chain vulnerability.

4. Objectives

The primary objectives of this assessment are to:

- Identify risks associated with the organization's third-party vendors.
- Develop a prioritized risk management plan aligned with NIS 2 requirements
- Provide actionable steps to achieve compliance and enhance supply chain security

By addressing these objectives, this report aims to support **EUS Cloud GmbH** in building a resilient and compliant cybersecurity framework.

Organizational Overview

1. Company Overview

EUS Cloud GmbH is a leading cloud service provider based in the European Union, specializing in infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and enterprise data storage solutions. Serving a diverse client base that includes healthcare providers, financial institutions, and public sector organizations, **EUS Cloud GmbH** plays a critical role in supporting operations across regulated industries.

2. Core Operations

The company operates a robust multi-cloud infrastructure that leverages a combination of proprietary technology and third-party services. Key operations include data hosting, application deployment, and cybersecurity monitoring. EUS Cloud GmbH relies heavily on third-party vendors for essential services such as:

- Data Centers: Hosting facilities managed by external providers.
- Software Tools: Applications used for service monitoring and client management
- Cybersecurity Solutions: External threat detection and vulnerability

3. Supply Chain Landscape

EUS Cloud GmbH works with over 30 vendors, categorized as:

- **Critical Vendors**: Providers whose services are essential for the company's operations, such as primary data centers and cybersecurity tools.
- **Non-Critical Vendors:** Providers whose services are auxiliary, such as marketing platforms and non-sensitive SaaS tools.

Given its reliance on vendors, supply chain security is critical to ensure uninterrupted service delivery and regulatory compliance. A single vulnerability in the supply chain could compromise sensitive client data or disrupt operations, leading to financial and reputational damage.

Methodology

1. Approach Overview

This assessment follows a structured approach aligned with the requirements of the NIS 2 Directive, focusing on evaluating and mitigating supply chain risks for EUS Cloud GmbH. The methodology ensures a thorough analysis of third-party vendors and their potential impact on the organization's overall cybersecurity posture.

2. Framework and Standards Used

- **NIS 2 Directive:** Specific articles addressing vendor risk management and reporting.
- **ISO 27001**: Guidelines for risk assessment and information security management.
- **ENISA Recommendations**: Best practices for securing supply chains in critical sectors.

3. Key Steps in the Assessment

a. Vendor Identification and Categorization

- Collected a list of 30+ third-party vendors
- Categorized vendors into critical and non-critical

b. Vendor Risk Evaluation

- Assessed vendors compliance with NIS 2 requirements, including their security controls, incident response readiness, and data protection policies.
- Used a standardized checklist to evaluate cybersecurity practices.

c. Risk Analysis

- Analyzed potential vulnerabilities using a Likelihood x Impact matrix.
- Categorized risks as Critical, High, Medium, or Low.

d. Prioritization

- Identified high-risk vendors whose vulnerabilities pose the greatest threat to business continuity and compliance.

e. Recommendations and Roadmap Development

- Developed actionable recommendations to address gaps in vendor compliance.
- Created a step-by-step roadmap for EUS Cloud GmbH to enhance supply chain security.

f. Tools and Techniques

To ensure a comprehensive and structured assessment, a combination of industry-recognized frameworks, automated tools, and manual evaluation methods were used. These tools facilitated data collection, risk analysis, and compliance evaluation of third-party vendors.

Frameworks and Standards Used:

- **NIS 2 Directive** – Served as the primary compliance benchmark, ensuring all risk assessments aligned with EU regulatory requirements.
- **ISO 27001** – Provided a structured approach to risk management and vendor security evaluation.
- **ENISA Supply Chain Security Guidelines** – Used as a reference for best practices in third-party risk management.

Risk Assessment and Compliance Evaluation Tools:

Tool	Purpose
Microsoft Office Suite	Used for **risk scoring, compliance checklists, vendor assessments** and generating the report.
Lucidchart	Created **vendor dependency** figures to visualize critical vendor relationships.

Risk Analysis & Prioritization Methods

- **Likelihood x Impact Risk Matrix** – Used to categorize risks as **Low, Medium, High, or Critical** based on severity and probability.

Findings

1. Overview of Findings

The supply chain cybersecurity risk assessment for **EUS Cloud GmbH** identified several critical vulnerabilities and compliance gaps across its third-party vendor ecosystem. These issues range from insufficient incident response capabilities to inadequate data protection measures. Of the 30 vendors assessed:

- 73% were fully compliant, demonstrating robust cybersecurity practices
- 10% were partially compliant, with significant gaps in critical areas
- 17% were found to be non-compliant with NIS 2 requirements

The findings highlight the need for **EUS Cloud GmbH** to strengthen vendor oversight, enhance contractual agreements, and prioritize remediation efforts for high-risk vendors

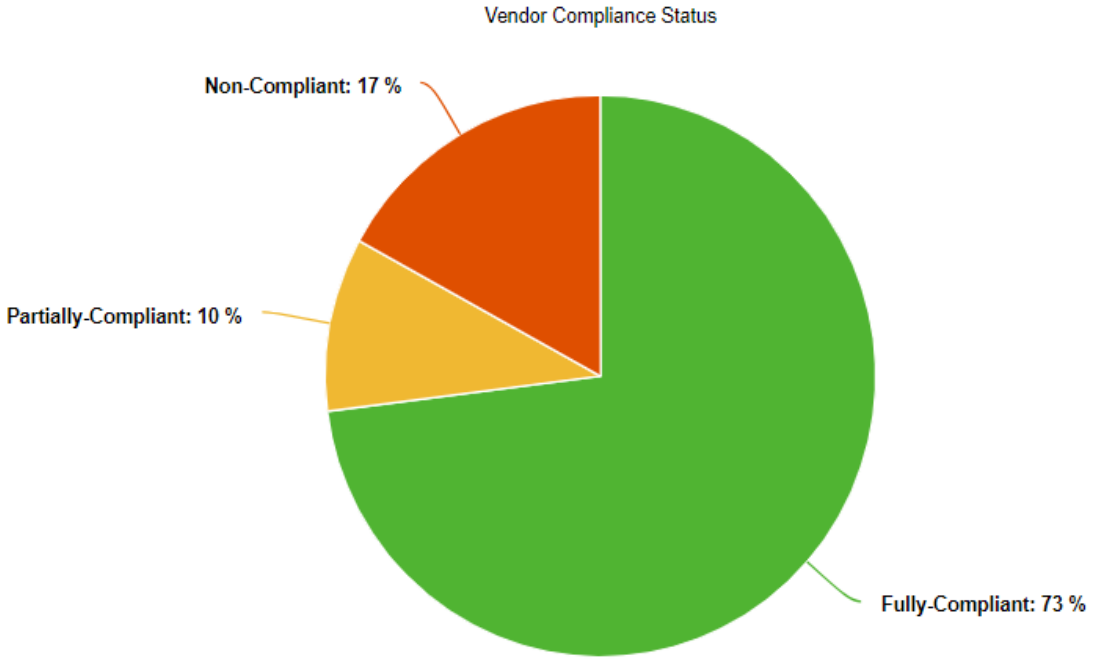

Figure 1: Vendor Compliance Status

2. Detailed Findings

Vendor Name	Category	Compliance Status	Key Issues	Service/Risk	Impact Level
Vendor A	Critical Vendor	Non-Compliant	No documented incident response plan.	Provides data center services; a breach could disrupt client operations and lead to financial loss.	High
Vendor B	Critical Vendor	Non-Compliant	Outdated software with known vulnerabilities.	Offers a cloud-based backup service; unpatched software increases exposure to ransomware attacks.	High

Vendor C	Non-Critical Vendor	Non-Compliant	Encryption is not applied to sensitive data in transit.	Provides a SaaS analytics tool; lack of encryption could expose data during transmission.	Medium
Vendor D	Critical Vendor	Non-Compliant	Weak access controls	Supplies a security monitoring tool; unauthorized access could lead to tampering with threat detection capabilities.	High
Vendor E	Critical Vendor	Partially Compliant	Incident notification times exceed 48 hours	Provides cybersecurity monitoring services; delayed reporting could lead to prolonged attacks.	High
Vendor F	Non-Critical Vendor	Partially Compliant	No periodic vendor security audits or supply chain risk evaluations.	Provides enterprise collaboration software; lack of auditing could allow undetected vulnerabilities to persist.	Medium

Table 1: Detailed Compliance Findings

3. Key Vulnerabilities Identified

a. Lack of Incident Response Plans

- Issue: 2 out 5 non-compliant vendors lacked formalized incident response mechanisms.
- Example: A critical vendor managing data centers had no 24-hour incident notification or root cause analysis process.
- Impact: Failure to detect and mitigate attacks quickly could lead to prolonged downtime, regulatory violations, and reputational damage.

b. Outdated and Unpatched Software

- Issue: 1 non-complaint vendor relied on outdated software with known vulnerabilities.
- Example: A backup service provider had unpatched systems, making them susceptible to ransomware threats.
- Impact: Unpatched vulnerabilities increase the risk of cyberthreats targeting critical infrastructure.

c. Weak Access Control

- Issue: 2 partially compliant vendors lacked robust access control measures.
- Examples: A security monitoring vendor used shared administrative credentials instead of role-based access control (RBAC)
- Impact: Unauthorized access could lead to compromised system integrity and data breaches.

d. Delayed Incident Reporting

- Issue: 1 partially compliant vendor failed to meet the NIS 2 mandated 24-hour notification requirement.
- Example: A cybersecurity monitoring vendor reported incidents after 48 hours, delaying response actions.
- Impact: Prolonged incident resolution could exacerbate security breaches and increase recovery costs.

4. Supply Chain Risk

- **Regulatory Non-Compliance:** Non-compliant vendors expose the organization to potential penalties under NIS 2, including fines up to €10 million or 2% of global turnover.
- **Operational Disruptions:** Vendor-related security incidents could impact business continuity, particularly in cloud hosting and data center operations.
- **Reputational Damage:** A supply chain breach could lead to loss of client trust, particularly in regulated industries like finance and healthcare.
- **Financial Impact:** Security failures could lead to fines, lawsuits, and increased cybersecurity costs for remediation efforts.

Risk Assessment

1. Introduction

This section categorizes and prioritizes the supply chain security risks identified in the findings. The goal is to assess risks based on their likelihood of occurring and their impact on **EUS Cloud GmbH**'s operations. This structured risk assessment will help prioritize mitigation efforts and ensure compliance with **NIS 2** requirements.

To quantify risk, each vulnerability is assessed using a **Likelihood x Impact** model, where:

- **Likelihood** measures how often the risk is expected to occur.
- **Impact** assesses the severity of the consequences if the risk materializes.

2. Compliance Overview

Before diving into risk scoring, we first review the compliance levels among third-party vendors. The assessment found that:

- 73% (22 vendors) were fully compliant.
- 10% (3 vendors) were partially compliant.
- 17% (5 vendors) were non-compliant.

3. Risk Categorization

- Likelihood Scale (How often the risk might occur)
  - Rare (1) | Unlikely (2) | Possible (3) | Likely (4) | Almost Certain (5)
- Impact Scale (How Severe the Consequences Would Be)
  - Low (1) | Medium (2) | High (3) | Critical (4) | Severe (5)

Using this framework, the **Risk Matrix below** maps each risk into a **color-coded grid**.

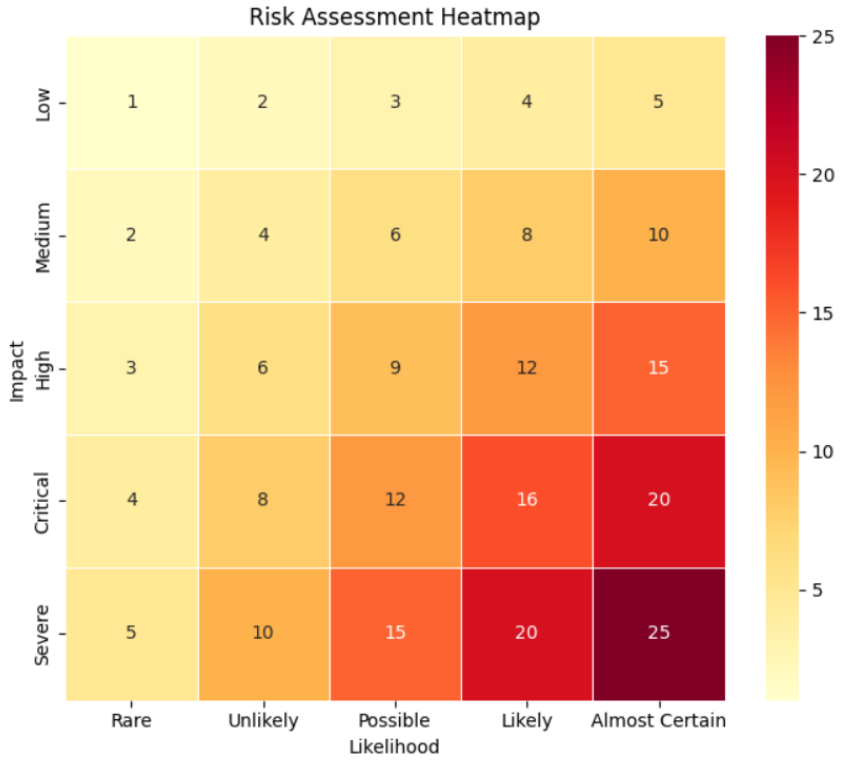

Figure 2: Risk Assessment Heatmap

4. Risk Prioritization Table

The following table ranks identified risks based on the risk assessment map, ensuring high-priority issues are addressed first:

Risk	Score (Likelihood × Impact)	Priority Lever
Lack of Incident Response Plan	**16** (4 x 4	**Urgent**
Outdated & Unpatched Software	**9** (3 × 3)	**High**
Weal Access Controls	**12** (4 × 3)	**High**
Encryption Gaps in Data Transit	**6** (3 x 2)	**Medium**
Delayed Incident Reporting	**6** (2 × 3)	**Medium**

Table 2: Risk Prioritization

5. Key Insights & Takeaways

- **Urgent Risks:** The lack of incident response plans is the most severe risk, requiring immediate remediation.
- **High-Priority Risks:** Unpatched software and weak access controls expose the company to major threats.
- **Medium-Priority Risks:** Encryption gaps and delayed incident reporting should be monitored but do not pose immediate threats.

Recommendations

1. Overview

This section outlines actionable steps for **EUS Cloud GmbH** to mitigate the risks identified in the Risk Assessment and ensure compliance with the **NIS 2** Directive. These recommendations are prioritized based on the Risk Prioritization Table, focusing on high-impact and high-likelihood risks first.

2. Strategy for Risk Mitigation

To ensure effective supply chain cybersecurity, **EUS Cloud GmbH** should take a multi-layered approach:

- **Immediate Action**: Addressing Urgent Risk
- **Short-Term Action**: Mitigating High Priority Risk
- **Long-Term Action**: Strengthening Vendor Compliance Checks

3. Actionable Recommendations Table

Risk	Mitigation Strategy	Timeline	Responsible Party
Lack of Incident Response Plan	– Require vendors to submit a documented **Incident Response Plan (IRP)**. – Establish **24-hour reporting** for critical incidents. – Conduct **tabletop exercises** to test vendor response.	Immediate (0–3 months)	Compliance & Security Team
Outdated and Unpatched Software	– Implement vendor patching policy in all contracts. – Conduct quarterly patch audits. – Enforce penalties for vendors failing to patch critical vulnerabilities.	Short-Term (3-6 months)	IT & Vendor Management Team
Weak Access Controls	– Require vendors to adopt Role-Based Access Control – Enforce Multi-Factor Authentication for all vendor systems.	Short-Term (3-6 months)	It Security Team

	– Conduct annual access reviews		
Encryption Gaps in Data Transit	– Mandate end-to-end encryptions for all sensitive data.	Medium-Term (6-9 months)	Compliance & Legal Team
Delayed Incident Response	– Implement a 24-hour mandatory incident reporting clause in vendor contracts – Introducing penalty clauses for late reporting – Establish a centralized incident reporting portal for vendors	Medium-Term (6-9 months)	Risk & Compliance Team

Table 3: Recommendation Table

4. Long-Term Vendor Risk Management Strategy

Beyond the immediate risk mitigation steps, **EUS Cloud GmbH** should establish long-term policies to maintain a secure and compliant vendor ecosystem:

- Vendor Security Rating System
- Annual Vendor Audits & Compliance Reviews
- Automated Vendor Risk Monitoring

Compliance Roadmap

Phase	Key Actions	Timeline
Phase 1: Immediate Actions *(0–3 Months)*	– Require vendors to submit **Incident Response Plans (IRPs)**. – Implement a 24-hour mandatory incident reporting policy Conduct a high-risk vendor review	0-3 Months
Phase 2: Strengthening Controls *(3–6 Months)*	– Enforce Role-Based Access Control (RBAC) & Multi-Factor Authentication (MFA). – Implement a vendor patching policy with compliance enforcement. – Require end-to-end encryptions for all sensitive data.	3-6 Months
Phase 3: Continuous Monitoring & Audit *(6–12 Months)*	– Establish annual vendor audits – Introduce a vendor security rating system – Implement automated risk monitoring tools for supply chain threats	6-12 Months

Table 4: Compliance Roadmap Table

5. Key Milestones

- Establishing a vendor compliance team
- 24-hour reporting enforced
- Vendor IRP (Incident Response Plan) collected
- MFA and Encryption fully implemented
- First annual vendor audit completed

Conclusion

1. Summary of Findings and Key Takeaways

The supply chain cybersecurity risk assessment for **EUS Cloud GmbH** has identified key vulnerabilities among third-party vendors, highlighting areas where security improvements are necessary to comply with the **NIS 2 Directive**.

Key takeaways of the assessment:

- **73%** of vendors are fully compliant, demonstrating strong cybersecurity practices.
- **10%** of vendors are partially compliant, requiring targeted security enhancements.
- **17%** of vendors are non-compliant, posing potential risks to regulatory compliance, operational resilience, and data security.

The most critical risks identified include:

- Lack of incident response planning among vendors
- Weak access controls and shared administrative credentials
- Outdated and unpatched software, increasing exposure to cyber threats
- Inconsistent encryption practices, leaving sensitive data vulnerable

2. Recommendation for Long-term Security

To mitigate these risks and ensure full **NIS 2 compliance**, EUS Cloud GmbH must implement:

- **Stricter Vendor Security Requirements**: Enforce stronger cybersecurity obligations in all vendor contracts.
- **Continuous Monitoring & Audits**: Conduct annual vendor security audits and require periodic compliance reviews.
- **Automated Risk Management**: Implement real-time monitoring tools to detect supply chain risks proactively.

3. Final Thoughts

The evolving cyber threat landscape requires a proactive approach to third-party risk management. As supply chain attacks continue to rise, organizations like **EUS Cloud GmbH** must establish continuous oversighting mechanisms to ensure long-term resilience.

By following the Compliance Roadmap outlined in this report, **EUS Cloud GmbH** will not only align with **NIS 2** Directive requirements but also strengthen trust with clients and stakeholders.

Appendices

The Appendices provide additional resources, templates, and supporting materials referenced in the report. These documents ensure that **EUS Cloud GmbH** has actionable tools to implement the recommendations effectively.

1. Vendor Compliance Checklist

A structured Vendor Compliance Checklist to evaluate third-party vendors against **NIS 2 requirements**.

Checklist Example:

Control Area	Requirement	Compliant (✓/✗)	Notes
Incident Response	The vendor has a documented IRP.		
Access Control	Enforces RBAC & MFA.		
Patch Management	Implements timely security updates.		
Encryption	Use E2E encryption for data.		
Incident Reporting	Reports incidents within 24 hours.		

Table 5: Checklist Example

2. Risk Assessment Template

Risk	Likelihood	Impact	Score (L x I)	Priority
[Risk]	[1-5]	[1-5]	[Auto Calculated]	[Low/Medium/High]

Table 6: Risk Assessment Template

3. Vendor Incident Response Plan (IRP) Template

A standardized IRP template for vendors to submit to **EUS Cloud GmbH**, ensuring compliance with **NIS 2** incident response requirements.

- **Incident Classification** – Define severity levels (Low/Medium/High/Critical).
- **Detection & Response** – Outline who, what, when, and how incidents are managed.
- **Reporting Procedures** – Vendors must notify EUS Cloud GmbH within 24 hours.
- **Recovery & Lessons Learned** – Root cause analysis and mitigation actions

4. References and Supporting Documents

A list of regulations, frameworks, and industry guidelines used to develop this report.
Key References:

- **NIS 2 Directive (EU 2022/0383)** – Official European cybersecurity regulation
- **ISO 27001** – Information Security Management System (ISMS) standard.
- **ENISA Guidelines** – European cybersecurity best practices for supply chain security.
- **OWASP Top 10 for Supply Chain Security** – Industry-recognized risks and mitigation strategies.