UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

A Framework for Assessing the Supply Chain Cybersecurity Risk Management Maturity

Rui Pedro Carvalho Diogo

Mestrado em Segurança Informática

Dissertação orientada por:
Profª. Doutora Ana Luisa do Carmo Correia Respício

2025

In memory of my grandfather, whose presence I'll always miss and whose love I'll always keep.

Acknowledgments

I would like to express my deep gratitude to all the professors that supported me during my Master's in information security but specially to my supervisor, Professor Ana Respício, for her invaluable guidance and support throughout the entire process of researching and writing this thesis. It was truly an honor to have the opportunity to learn from her.

I am truly grateful to the person who generously shared their time and expertise during the interview, as well as for the valuable opinions and insights they provided.

I would also like to thank my family, especially my mother Filomena and my father Joao, who fully supported me in all of my decisions and are always there for me. I wouldn't be who and where I am today without their love and guidance. I would also like to thank my brother Diogo, the person I always looked up to and who will forever be a reference for the person I want to be.

To those who have been with me since my first day at FCUL, you have my deepest appreciation: Costinha, Vski, and especially Afonso, who joined me in one of the most unforgettable experiences of my life, Erasmus.

To my longtime friend André, whose unwavering support has guided me throughout my life; his contribution to this work was no exception, he has truly been a pillar in my life.

Finally, I would like to thank two of my newest but most important friends: Sara, who stood by me throughout the journey of my thesis, sharing in all the ups and downs along the way, and Eduardo, who has always encouraged and supported me, both personally and professionally. Without a doubt, these past two years are the ones in which I grew the most, and it's mostly thanks to you both.

This work was partially supported by project no. 2024.07506.IACDC, DOI: 10.54499/2024.07506.IACDC, funded by measure RE-C05-i08.m04 – "Support the launch of an R&D project program aimed at the development and implementation of advanced cybersecurity, artificial intelligence and data science systems in public administration, as well as a scientific capacity building program", of the Recovery and Resilience Plan – PRR, under the financing contract signed between the Recover Portugal Mission Structure (EMRP) and the Foundation for Science and Technology I.P. (FCT), as an intermediate beneficiary.

Resumo

As cadeias de abastecimento evoluíram de estruturas lineares e relativamente simples para redes globais, interligadas e altamente complexas. Este fenómeno deve-se, em grande parte, à globalização, à transformação digital e à crescente externalização de serviços e processos para terceiros. Atualmente, uma organização raramente depende apenas dos seus recursos internos e, por consequente, a aquisição de produtos e serviços é feita através de múltiplos fornecedores, que por sua vez recorrem a outros parceiros, criando cadeias em vários níveis. Este ecossistema de interdependências, apesar de trazer vantagens económicas e operacionais, introduz também novos riscos, especialmente no domínio da cibersegurança. A interconectividade entre diferentes parceiros significa que uma vulnerabilidade num fornecedor pode comprometer toda a rede. Os atacantes exploram cada vez mais esta realidade, procurando pontos de entrada em entidades consideradas "elos fracos" e, a partir daí, propagando ataques a outras organizações pertencentes a cadeia. Os impactos resultantes de um ataque podem assumir proporções significativas, traduzindo-se em indisponibilidade operacional, violação da confidencialidade da informação, danos reputacionais e potenciais penalizações jurídicas.

Perante este contexto, é fundamental que as organizações vão além da implementação de controlos de segurança pontuais e adotem uma abordagem estruturada e integrada de gestão de riscos em toda a cadeia de abastecimento. Neste sentido, o presente trabalho tem como foco a avaliação e o reforço da maturidade da gestão de riscos de cibersegurança nas cadeias de abastecimento, propondo um modelo que auxilia as organizações a identificar o seu nível de maturidade atual e a definir medidas concretas para alcançar níveis superiores de maturidade.

O enquadramento teórico do trabalho assenta em três eixos principais, sustentados por normas internacionais que servem de base ao desenvolvimento metodológico. No domínio da cibersegurança, destacam-se as normas ISO/IEC 27001:2022, ISO/IEC 27002:2022 e ISO/IEC 27000:2018: a primeira estabelece requisitos para a gestão da segurança da informação e da privacidade, a segunda aborda a gestão de relações com terceiros e a terceira fornece terminologia e definições essenciais. Relativamente às cadeias de abastecimento, recorrem-se às normas ISO/IEC 15408-1:2022 e ISO/IEC 27036 (partes 1 a 3), que tratam da segurança nas relações cliente-fornecedor. No eixo da gestão de riscos, a investigação baseia-se nas normas ISO/IEC 27005:2022 e ISO/IEC 31000:2018, que definem o processo de identificação, análise, avaliação e tratamento de riscos, fornecendo orientações aplicáveis a diferentes contextos organizacionais. Para além destes três eixos principais, é ainda considerado o conceito de auditoria, apoiado na norma ISO/IEC

19011:2018, que fornece diretrizes para auditorias a sistemas de gestão. Embora não constitua um dos eixos principais, é apresentado por ser uma parte fundamental do modelo.

A revisão da literatura demonstra que, apesar da consolidação de normas internacionais e da existência de modelos desenvolvidos para cada um dos eixos centrais — cibersegurança, gestão de riscos e gestão de relações cliente-fornecedor — subsiste uma fragmentação significativa na sua aplicação integrada ao contexto real das cadeias de abastecimento. Esta limitação traduz-se numa utilização isolada de práticas, que frequentemente não reflete a complexidade dos ecossistemas. Entre os fatores críticos identificados nas cadeias de abastecimento destacam-se a necessidade de assegurar um alinhamento consistente entre objetivos estratégicos e medidas de segurança, bem como de promover níveis elevados de transparência e visibilidade ao longo de múltiplos níveis da cadeia.

A crescente complexidade destas redes, marcada pela multiplicidade de atores e pela intensidade dos fluxos de informação, potencia a emergência de novos pontos de vulnerabilidade que carecem de uma abordagem coordenada. Neste enquadramento, diversos modelos de referência têm procurado dar resposta, sendo o modelo SCOR um dos mais relevantes pela sua capacidade de mapear processos e apoiar a tomada de decisão de todos os intervenientes da cadeia. Paralelamente, a literatura sublinha a importância da formalização de requisitos contratuais, conforme estabelecido pela norma ISO/IEC 27036, que distingue os diferentes tipos de relações e especifica os respetivos mecanismos de proteção da informação. Adicionalmente, são apresentados modelos de gestão de riscos e de maturidade que, ao serem adaptados e integrados, servem de base ao desenvolvimento do modelo proposto neste trabalho.

Dando seguimento à análise, apresenta-se o modelo conceptual desenvolvido, concebido para integrar de forma coerente e operacional os diferentes referenciais teóricos previamente explorados. Este modelo estrutura-se em fases sequenciais e complementares, possibilitando às organizações adotar uma abordagem sistemática à maturidade da gestão de riscos na cadeia de abastecimento. A fase inicial corresponde a um momento de diagnóstico, no qual se avaliam as condições existentes, nomeadamente o nível de maturidade atual, a resiliência organizacional e o grau de alinhamento entre as partes interessadas. Nesta etapa assume particular relevância o mapeamento das relações cliente-fornecedor e a caracterização dos fluxos de informação e de responsabilidade que atravessam os vários níveis da cadeia. Este diagnóstico preliminar é fundamental para a identificação de lacunas, a compreensão dos principais desafios e a definição de bases sólidas para a implementação subsequente do modelo. As lacunas identificadas orientam a tomada de decisão relativamente aos ativos que requerem intervenção, sendo esse processo apoiado no modelo SCOR, o qual permite estruturar um plano de ação suportado por métricas de maturidade.

Com base no diagnóstico inicial, a organização avança para a definição de mecanismos formais de identificação, análise e avaliação de riscos. A fase de identificação é realizada através de processos estruturados de seleção de fornecedores, nos quais estes submetem as suas propostas em conformidade com os requisitos de segurança previamente estabelecidos, assegurando que a dimensão da cibersegurança é considerada desde o início da relação contratual. Segue-se a fase de

análise, na qual cada candidato é avaliado por meio de métodos qualitativos que ponderam simultaneamente a natureza da relação contratual a estabelecer e o nível de maturidade em segurança atribuído, correspondente aos selos de maturidade. Esta combinação permite determinar o grau de preparação de cada fornecedor e, em articulação com a avaliação do impacto potencial de um incidente, calcular o nível de risco associado. Por fim, a fase de avaliação consiste na tomada de decisão informada, que poderá traduzir-se na aceitação do risco identificado ou, em alternativa, no avanço para a contratação e subsequente progressão para a fase seguinte do processo.

Concluído o processo de apreciação de riscos, segue-se a fase de celebração contratual, na qual, para além da incorporação dos processos anteriormente identificados na literatura, a definição de métricas de auditoria assume um papel central. Estas métricas constituem instrumentos fundamentais para monitorizar o cumprimento dos requisitos estabelecidos e, simultaneamente, fornecer indicadores objetivos que permitem mitigar as fragilidades associadas à transparência e à visibilidade na cadeia de abastecimento.

A aplicabilidade prática do modelo foi demonstrada através de um caso de uso conceptual, inspirado na realidade de uma empresa multinacional do setor das tecnologias de informação, no qual os diferentes elementos do modelo foram analisados e exemplificados de forma operacional, aproximando a proposta à realidade organizacional. Para avaliar a framework desenvolvida, realizou-se uma entrevista com uma especialista em gestão de ciber risco da cadeia de abastecimento de IT, cujo contributo forneceu perspetivas críticas valiosas e destacou a necessidade de pequenos ajustes para o reforço adicional do modelo.

Num contexto económico global caracterizado por uma crescente interconectividade, em que uma falha localizada pode desencadear consequências sistémicas em toda a rede, a adoção de controlos isolados ou de medidas meramente reativas revela-se manifestamente insuficiente. Torna-se, por isso, essencial a implementação de abordagens integradas, colaborativas e sustentáveis, capazes de acompanhar a evolução constante das ameaças e os desafios inerentes à transformação digital. O modelo proposto neste estudo procura dar resposta a estas exigências, colmatando lacunas identificadas na literatura e apresentando uma estrutura conceptual que permite às organizações avaliar de forma sistemática o seu nível de maturidade e delinear estratégias para o reforço da maturida de gestão de riscos de cibersegurança nas cadeias de abastecimento.

Palavras-chave: Cadeia de Abastecimento; Gestão de Risco; Cibersegurança; Maturidade; Auditoria

Abstract

Supply chains have developed into complex, multi-tiered global networks, creating challenges for companies to maintain full visibility and implement risk management across all levels. Attackers increasingly target third parties viewed as weak links, using them as entry points to infiltrate and spread throughout the network. This can lead to system downtime, exposure of sensitive information, and reputational damage. When one link in the chain is compromised, the entire network may be at risk, especially with today's heightened connectivity between partners, making strong security measures more critical than ever.

This study proposes a supply chain cybersecurity risk management maturity framework for organizations that want to improve transparency, alignment, and trust between suppliers, safeguard assets, and advance the maturity of their cybersecurity risk management process. While research has addressed these areas separately, a practical solution that incorporates all of these areas is hard to find.

The framework is built on adaptable steps suitable for companies of any size or location, it integrates the SCOR Model as a reference aid in decision-making, a standards-aligned risk management process that incorporates maturity seals, an audit layer, and KPI-driven continuous monitoring. Through this integration, the framework delivers a consistent assessment baseline, transparent supplier evaluation, and an improvement roadmap to enhance supply chain cybersecurity risk management maturity. The framework was validated through evaluation by a specialist, whose feedback helped improve its adaptability across a wider range of contexts.

Keywords: Supply chain; Cybersecurity; Risk Management; Maturity; Auditing

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter outlines the motivation for exploring supply chain cybersecurity risk management maturity, the objectives and general methodology of the work, its key contributions, and the overall structure.

1.1 Motivation

As our digital ecosystem becomes increasingly interconnected, the risk from supply chain cyber incidents and compromises is growing, so organizations must prioritize transparency, resilience, and robust cybersecurity measures within their supply chains to mitigate these risks [18]. Since cybersecurity risks in the supply chain extend beyond information and communication technology (ICT) services or infrastructure providers and affect all organizational areas with digital interactions, addressing these persistent cyber threats requires a company-wide approach driven by business objectives to mitigate the significant risks involved.

The trend toward using supplier-managed services over in-house enterprise software has heightened the need for businesses to closely monitor both direct and indirect suppliers within their supply chains. These suppliers often require privileged access to manage services or equipment, and the reliance on external services introduces additional applications and services for deployment, management, and security. This expanded network of suppliers increases the potential attack surface for cyber threats [7]. Malicious actors may exploit this by targeting a vulnerable supplier within the chain, circumventing the robust defenses of a primary organization and gaining access to other connected entities, thus increasing the risk of widespread damage across the supply chain [58].

It is crucial to recognize that while strides have been made in cybersecurity, the specific nuances of supply chain cybersecurity, especially when it comes to supply chain risk management maturity, remain relatively unexplored [41]. The intersection of supplier-managed services, privileged access, and the intricate network of digital interactions within supply chains presents a unique set of challenges.

Therefore, this research seeks to contribute to this under-explored domain by providing an understanding of the dynamics involved and developing a strategy that will aim to fortify supply

chains against cyber threats. Building on this foundation, we are aiming to develop a framework for supply chain risk management maturity that identifies, evaluates, and mitigates potential risks posed by third-party vendors and suppliers.

1.2 Objectives

The primary goal of this work is to develop a comprehensive framework for supply chain cybersecurity risk management maturity (SCCRMM), with focus on critical but often-neglected areas such as transparency and trustworthiness among chain members [46]. By implementing practical, holistic strategies, this framework aims to strengthen cybersecurity risk management practices throughout the supply chain, ultimately elevating the entire chain's risk management maturity.

The goals of this work also include:

- Analyze the varying impacts of direct suppliers and the suppliers who supply them, and explore ways to address this escalation on wider chains.
- Explore the challenges of information security in supply chains, where both acquirers and suppliers are crucial to managing risks. This involves examining the acquirers responsibility to evaluate suppliers and mitigate risks when acquiring hardware, software or services.
- Understanding the challenges in supply chains, including the increase in attack vectors and the broader range of vulnerabilities within complex, global networks, as well as the critical importance of detailed contracts between suppliers and acquirers.
- Emphasize the importance and impact of conducting regular risk assessments among all members of the supply chain.

1.3 Contributions

The framework is designed to assist organizations in staying aligned with technological advancements, adapting to shifting business needs, and enhancing their market position. It also offers a clear, straightforward path to achieving the desired level of risk management maturity within the supply chain, built upon well established and recognized standards and models, including ISO/IEC, NIST and Maturity Seals.

In conclusion, the research, particularly the developed framework, is a valuable contribution not only to organizations but also to the field of supply chain cybersecurity for the following reasons:

- Highlights the necessity for a comprehensive methodology applicable to all IT supply chains.
- Emphasizes the importance of clear cybersecurity contractual requirements among supply chain partners

- Establishes a structured maturity framework to enhance the cyberscurity risk management process within the supply chain
- Aids in decision-making when acquiring suppliers.

1.4 Methodology and Timeline Overview

As demonstrated in Figure 1.1, several essential phases were undertaken, including the investigation and analysis of bibliographic references related to the topic, the development of a methodological framework to achieve the outlined objectives, and the administration of a questionnaire ir order to evalute the framework.

These steps are designed to assess the viability of the proposed model and identify potential challenges for future research. After reviewing related works and conducting a contextual analysis, the model was developed. Criteria were then established to evaluate supply chain risk management and, in turn, advance risk management maturity, ensuring alignment with the model's objectives.

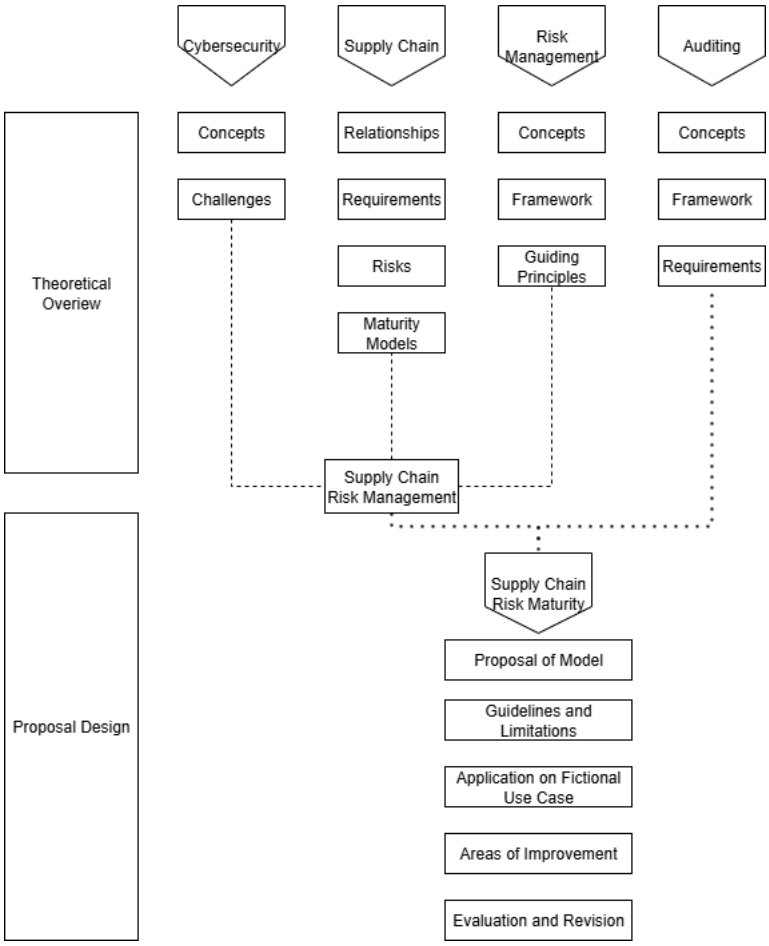

Figure 1.1: Research strategy

Building on the insights gathered during the research phase, the objective was to develop a model capable of addressing the identified gaps and meeting the defined requirements. To

strengthen the model's structure and ensure its practical relevance, standards and industry frameworks of risk management and auditing were incorporated within the context of the supply chain. Additionally, an interview was designed and administered to experts profiles, with the aim of validating the model and reinforcing the overall quality and applicability of the work produced.

1.5 Structure and Organization

This document is structured as follows:

- **Chapter 2 – Background**. This chapter introduces the fundamental concepts relevant to the theme of this work, establishing a foundation for understanding key topics such as information security, risk management, and supply chain dynamics.
- **Chapter 3 – Related Work**. This chapter reviews existing studies within the scope of the theme, highlighting the critical importance of supply chain cybersecurity with a focus on risk management practices.
- **Chapter 4 – Framework**. This chapter presents and details the framework developed to address supply chain cybersecurity risk management maturity.
- **Chapter 5 – Analysis and Evaluation**. This chapter presents a fictional use case to demonstrate the proposed framework, evaluate its effectiveness and practicality, and review the framework in light of this evaluation.
- **Chapter 6 – Conclusion and Future Work**. This chapter summarizes the key findings of the research, reinforces the main contributions of the work, and reflects on the overall relevance and impact of the proposed model.

Chapter 2

Background

This chapter presents the essential concepts of cybersecurity supply chain risk management, establishing the foundation for understanding risk management maturity and the proposed model. In addition, it introduces auditing as a necessary concept that will be incorporated into the model. To facilitate a comprehensive understanding, the chapter will be divided into three parts of the title:

- **Cybersecurity:** guided by the ISO/IEC 27001:2022[33], ISO/IEC 27002:2022[34], and ISO/IEC 27000:2018 standards[30], the approach addresses various aspects of information security. The first standard outlines requirements for information security, cybersecurity, and privacy protection, while the second focuses on managing third-party relationships. The third standard primarily deals with terminology and definitions.
- **Supply Chain:** centered on ISO/IEC 15408-1:2022[28] and ISO/IEC 27036[32, 36, 37] standards, which cover both cybersecurity and supply chain relationships,
- **Risk Management:** based on ISO/IEC 27005:2022[35] and ISO/IEC 31000:2018[31] standards, which define the risk management process and guidelines.
- **Auditing:** following ISO/IEC 19011:2018[29], which provides guidelines for auditing management systems.

This division provides a structured approach to understanding the interplay between cybersecurity, risk management, and supply chain dynamics.

2.1 Cybersecurity

2.1.1 Information Security

All information managed by an organization is exposed to various threats, including attacks, human errors, and natural disasters such as floods or fires, as well as vulnerabilities inherent in its use. Information security revolves around treating information as a valuable asset that requires adequate protection, particularly against risks to its availability, confidentiality, and integrity. Ensuring accurate and complete information is accessible promptly to authorized individuals serves as a critical driver for business efficiency.

Effectively protecting information assets by defining, implementing, maintaining, and improving information security is crucial for an organization to achieve its goals while upholding legal compliance and safeguarding its reputation. These coordinated efforts, which involve applying appropriate controls and addressing unacceptable information security risks, are commonly referred to as components of information security management[30].

2.1.2 Stakeholders

To examine the supply chain, it is essential to identify the key stakeholders and their roles in managing assets and mitigating risks, ISO/IEC 27002:2022[34] describes a stakeholder as a person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. According to the ISO/IEC 15048-1 standard [28], stakeholders are grouped into five categories, each with a vested interest in risk management:

- **Consumers (Risk Owners):** Use the result of both risk analysis and policies in order to help their decision making
- **Developers:** Makes sure that the security requirements are identified and met
- **Technical working groups:** May be composed of consumers, developers and/or evaluators, and they help in support and guidance
- **Evaluators:** Evaluate the level of conformity between assets and their risk criteria
- **Others:** Any entity with interest and/or responsibility such as auditors, designers, evaluation authorities,etc..

2.1.3 Assets

According to ISO/IEC 27002:2022 an asset[34] is anything that has value to the organization, and they are divided into two kinds:

- Primary Assets, that can be divided in:
  - Information
  - Business Processes and Activities
- Supporting Assests, such as:
  - Hardware
  - Software
  - Network
  - Personnel
  - Site
  - Organization Structure

Many assets exist as information that is stored, processed, and transmitted through IT products to fulfill the requirements established by their owners. These owners may demand strict controls

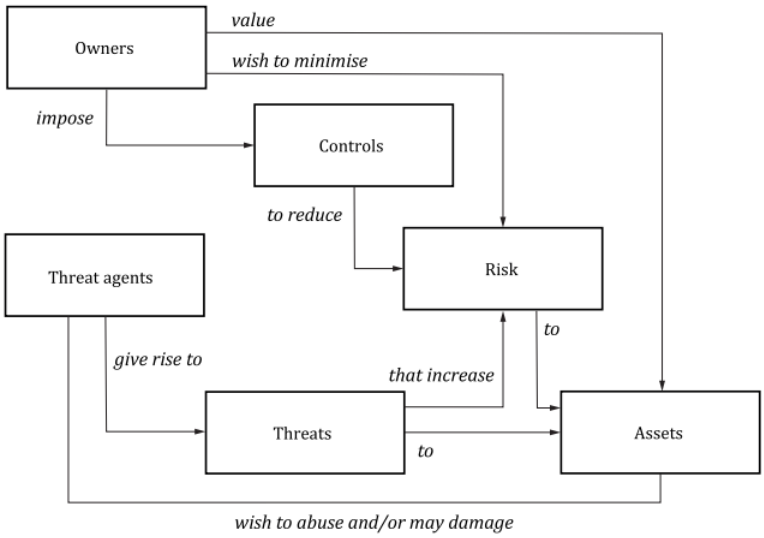

Figure 2.1: Cybersecurity concepts and relationships (extracted from ISO/IEC 15048-1:2022 [28])

over the availability, distribution, and modification of such information, ensuring that assets are shielded from threats through security measures implemented within the operational environment. Figure 2.1 represents these key concepts and their interrelations.

Safeguarding these assets falls under the responsibility of their owners, who determine their value and significance. However, these assets may also attract potential or actual threat agents aiming to exploit them in ways that oppose the owners' interests. Such threats represent potential risks that could jeopardize their assets, diminishing their overall value. Security compromises often manifest as breaches of confidentiality, violations of integrity, or disruptions to availability.

Asset owners are responsible for their assets and must be able to justify their decision to accept the risks of exposing them to potential threats. The standard[28] establishes an evaluation framework and relationship designed to enhance confidence in the effectiveness and suitability of the controls (Show in annex A.1).

2.1.4 Controls

A control is a measure intended to influence risk, either by reducing it or keeping it at an acceptable level. For example, an information security policy helps sustain risk within defined acceptance criteria, while consistently following that policy can actively lower the risk.

Organizations can design or adopt controls as needed, considering the resources and investment required relative to the business value they provide. A balance must be struck between the cost of implementing controls and the potential impact of security incidents without them. Risk assessment results should guide management actions, prioritize addressing security risks and determine necessary controls.

Controls are grouped into four categories, and their layout is defined in annex A.2:

- People
- Technological
- Physical
- Organizational

The determination of controls depends on the organization's decisions following a risk assessment within a clearly defined scope. Relevant national and international laws and regulations must also be considered. Additionally, controls should be assessed for how they interact to create a layered defense strategy[34].

2.2 Cybersecurity Risk Management

ISO/IEC 31000:2018[31] states that managing risk is an iterative process that supports organizations in setting strategies, achieving objectives, and making informed decisions. It is integral to governance and leadership, forming a core part of how an organization is managed at all levels and contributing to the enhancement of management systems. Embedded in all organizational activities, managing risk involves interaction with stakeholders and considers both external and internal contexts, including human behavior and cultural factors [25]. The components of risk management may already exist partially or fully within an organization but may require adaptation or improvement to ensure that risk management remains efficient and consistent.

An iterative process is specified in ISO 27005:2022[35] designed to manage information security risks effectively, building on the requirements outlined in ISO 27001:2002[33], each iteration improves the depth and precision of the risk assessment. This process helps organizations define their internal and external contexts, identify, analyze, and evaluate risks, and determine appropriate controls. The process continues until the risk assessment aligns with acceptable criteria, allowing decisions to either accept or modify the risks. Figure 2.2 demonstrates the process which has the following steps:

- **Context Establishment:** Defining the scope of the risk management process and understanding the internal and external factors that may impact the organization
- **Risk Assessment**
  - **Risk identification:** The process of finding, recognizing and describing risks. This involves the identification of risk sources and events.
  - **Risk analysis:** Points toward determining the level of the risk, this encompasses assessing potential consequences and the likelihood of the risk. The level of risk should be determined as a combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios.
  - **Risk Evaluation:** Evaluating and comparing the level of risks against risk evaluation criteria is essential to prioritize treatment, if needed.

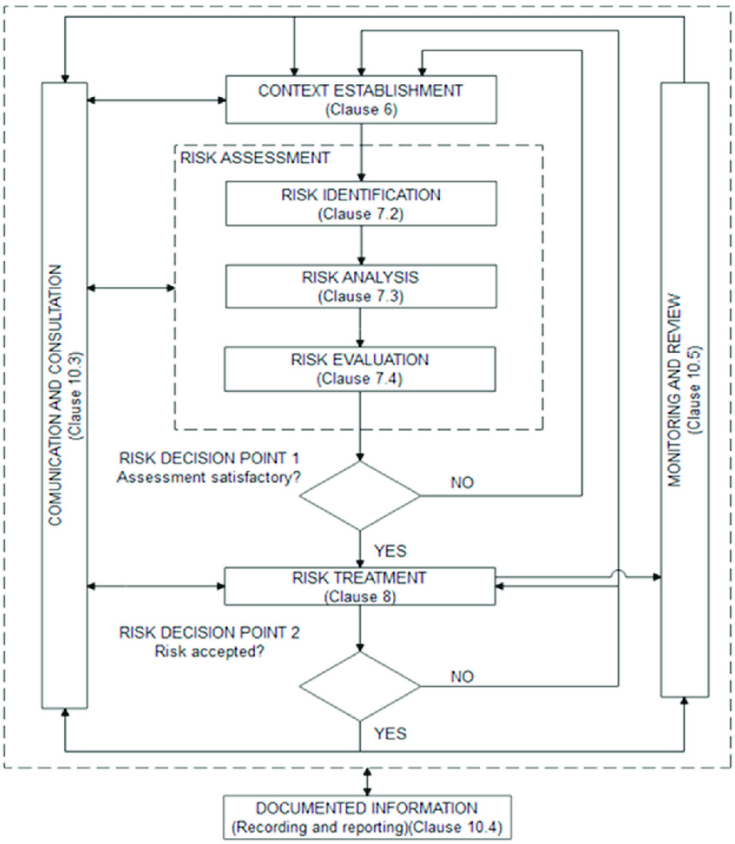

Figure 2.2: Information Security Risk Management process (extracted from ISO/IEC 27005:2022[35])

- **Risk Treatment:** Based on the risks prioritized in the assessment, the deployment or enhancement of security controls will be based on their relation, as outlined in the risk treatment plan.

- **Communication and Consultation:** Aims to achieve agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners and other relevant interested parties.

- **Monitoring and Review:** The goal is to ensure that risk treatments are effective, efficient, and economical in both their design and operation. Additionally, it aims to gather information to enhance future risk assessments.

- **Documented Information:** Information about the information security risk assessment and treatment processes.

For the framework, the emphasis is on the output of the risk assessment, particularly the risk analysis, where scenarios and the likelihood of risks are examined.

2.2.1 Risk Analysis: Level of Risk (Qualitative)

According to ISO/IEC 27005:2022[35] the effectiveness of qualitative scales and the reliability of the risk assessments based on them depend entirely on the consistent interpretation of category labels by all stakeholders. To achieve this, the levels of a qualitative scale must be unambiguous, with clearly defined increments, objective descriptions for each level, and non-overlapping categories.

Therefore, verbal descriptors of consequence (demonstrated in Annex A.1), likelihood (demonstrated in Annex A.2), or risk should be explicitly linked to unambiguous scales anchored in numerical or proportional reference points. All stakeholders must be informed about these reference scales to ensure consistent interpretation of qualitative assessment data and outcomes.

Table 2.1 represents a qualitative risk matrix:

Likelihood	Consequence				
	Catastrophic	Critical	Serious	Significant	Minor
Almost Certain	Very High	Very High	High	High	Medium
Very Likely	Very High	High	High	Medium	Low
Likely	High	High	Medium	Low	Low
Rather Unlikely	Medium	Medium	Low	Low	Very Low
Unlikely	Low	Low	Low	Very Low	Very Low

Table 2.1: Example of qualitative approach to risk criteria according to ISO/IEC 27005:2022[35]

2.3 Supply Chain

ISO/IEC 26036-1:2021[32] states that a supply chain consists of interconnected organizations that utilize shared resources and processes, with each entity serving as an acquirer, supplier, or both. These relationships are formed through purchase orders, agreements, or other formal sourcing arrangements. The supply chain may encompass vendors, manufacturing facilities, logistics providers, distributors, distribution centers, and other entities engaged in manufacturing, processing, design, development, product handling, and delivery. It also includes service providers responsible for the operation, management, and delivery of services.

Acquirers and suppliers can pose information security risks to one another [12]. Both parties must evaluate and address these risks by effectively managing information security and implementing appropriate controls.

2.3.1 Supply Chain Relationships

There are 3 types of supplier relationships:

- **Supplier relationships for products:** When an acquirer engages a supplier, information security risks can arise from shared access to sensitive data, product vulnerabilities, malfunctions, or unmet requirements. To manage these risks, the acquirer may control the

supplier's access to its information and oversee production processes. This oversight can also expose the supplier's information to the acquirer. To ensure product quality and security, the acquirer may require audits, monitoring, or certifications, with these measures agreed upon by both parties.

- **Supplier relationships for services:** When acquiring services, suppliers often access the acquirer's information, posing security risks, especially in business process outsourcing. Access may occur onsite, remotely, or at the supplier's location, influencing security controls. Acquirers should set rules to manage access and ensure service quality, often through service level agreements (SLAs). Monitoring, audits, or certifications can provide additional assurance, with all measures mutually agreed upon.

- **ICT supply chain:** The ICT supply chain consists of interconnected organizations involved in producing and delivering ICT products and services, often sourced from multiple suppliers. Each organization acts as an acquirer for upstream suppliers and a supplier for downstream customers, with the end customer having limited or no control over information security beyond their direct supplier. Information security risks are inherited throughout the supply chain, but managing these risks is challenging due to limited visibility and access to suppliers' suppliers [60].

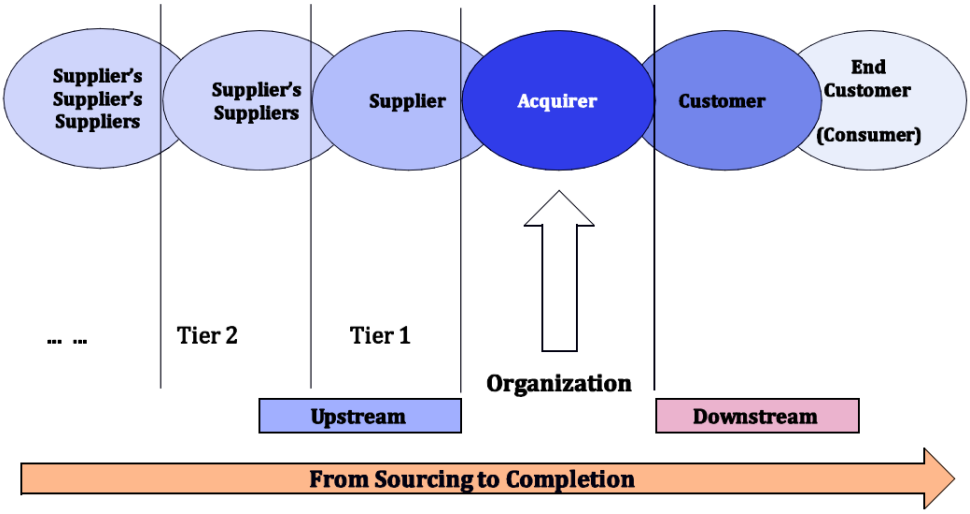

Figure 2.3: Supply Chain relationships (extracted from ISO/IEC 27036-1:2021[32])

As depicted in Figure 2.3, an organization in an ICT supply chain is an acquirer in relation to the upstream organization, and a supplier in relation with downstream organization. The adjacent downstream organization is often called a customer from the perspective of the organization that provides products or services to it. The customer at the end of the ICT supply chain is referred to as an end customer, or consumer.

2.3.2 Information Security in Supply Chain

Within the span of supply chains, safeguarding information security extends beyond the perimeters of individual organizations, whether they play the role of acquirer or supiplier.

Considering this, Control 5.19 from the ISO/IEC 27002:2022 standard [34] emphasizes that organizations must establish, communicate, and enforce policies and procedures to address security risks linked to supplier-provided products and services, including cloud-based solutions. Essential elements include:

1. **Policy Development and Communication:** Develop topic-specific supplier relationship policies and communicate them to relevant stakeholders.

2. **Supplier Management Process:** Ensures security risks are addressed throughout the supplier lifecycle. Organizations must identify critical suppliers, evaluate and select them based on security criteria, and define access to sensitive information and infrastructure. Risks from supplier personnel, products, and services must be assessed and managed, while compliance with security requirements is continuously monitored. Procedures for incident handling, resilience, and secure termination of relationships, including revoking access and safeguarding information, are essential. Staff training and secure transfer of information during supplier changes further support maintaining information security.

3. **Controls and Legal Requirements:** When suppliers cannot meet specific requirements, organizations must make risk-informed decisions and implement compensating controls to protect their information. Legal and contractual responsibility for information security always remains with the organization, even when services are outsourced. Risks from supplier access, cross-border data transfers, and inadequate ICT controls must be mitigated using measures like non-disclosure agreements, cryptographic techniques, and robust oversight.

2.3.3 Security Requirements

As organizations become more interconnected with third parties and the digital boundaries diminish, incorporating specific contractual clauses is vital to mitigate potential information security risks. These clauses must be thorough and customized to meet the relevant requirements of the third-party relationship. Controls 5.20 and 5.21 of ISO/IEC 27002:2022[34] build key contractual requirements necessary to ensure an agreed level of information security in supplier relationships, such as:

- **Create and document supplier agreements that outline mutual responsibilities** to meet the security requirements, such as:
  - Information handling
  - Legal Compliance
  - Controls Implementation
  - Authorization
  - Sub-Contracting
  - Disaster Recovery

  - Termination provisions
  - Information Transfer

.

- Maintain a register of supplier agreements to track information sharing.
- Periodically review and update agreements to ensure relevance and effectiveness.
- Define **specific security requirements for acquiring ICT products** and services and ensuring that suppliers apply these standards **throughout their supply chains**, including any subcontractors.
- Require suppliers to adopt and propagate security best practices in their supply chain, including subcontracted components.
- Critical components of ICT products and services that are **essential for functionality** should be **identified, especially if they involve outsourcing**. These components need thorough scrutiny, and assurance of authenticity and integrity.
- Organizations are encouraged to seek formal security certifications, to ensure ICT products meet required security levels.
- Rules for sharing supply chain information and addressing potential risks or compromises.
- Provisions for addressing component obsolescence or supplier discontinuity. This includes planning for alternatives, identifying backup suppliers, and ensuring a seamless transfer of resources if needed.

2.3.4 Monitoring and Review

The acquisition of hardware, software, and services introduces distinct information security risks that demand meticulous consideration. In the ever-evolving complexity of supply chains effective management of supplier services involves ensuring compliance with information security requirements, effectively handling incidents and problems, and mitigating risks arising from changes in supplier services or their business status [42]. This process, developed in control 5.22 on the ISO/IEC27002:2022[34], includes overseeing the organization-supplier relationship by taking the following actions:

- Monitoring Service Performance
- Monitor Supplier Changes
- Monitoring Service Changes
- Audit and Follow-Up
- Incident Management and Vulnerability Asessment
- Supplier Relationship and Compliance
- Evaluating Security Levels

A designated individual or team should be tasked with managing supplier relationships. They should have access to adequate technical skills and resources to ensure that the agreement's requirements, especially those related to information security, are being fulfilled [22].

2.3.5 Supply Chain Risks

The standard ISO/IEC27036-1:2021[32] states that the supply and support of a product or service often require the exchange of information and information systems between the acquirer and the supplier. To ensure the security of this shared information, it is essential to establish a formal agreement between the two parties [10]. This agreement should outline a mutually acceptable set of controls and clarify the responsibilities for their implementation [49]. Without such an agreement, the information security of either party could be compromised in the following ways:

- Differences in information security governance, risk tolerance, compliance practices, or organizational cultures between the acquirer and supplier can lead to gaps in security requirements and controls.
- Dependence on the supplier's services and capabilities to meet the acquirer's information security needs may create unintended dependencies on specific controls.
- Conflicting or misaligned security controls between the acquirer and supplier could weaken or interfere with the other party's overall information security.

Supplier relationships, previously introduced in Chapter 2.3.3, can pose significant information security risks to both acquirers and suppliers throughout their lifecycle. In this section, we will explore further into these relationships, mentioning key risks such as (More risk for acquiring both products and services are on Annex A.4):

1. **Lack or weakness of governance:** Acquirers lose control over how their information is stored, processed, transmitted, created, modified and destroyed.
2. **Miscommunication and misunderstanding:** Controls put in place by the supplier do not address the risks identified by the acquirer, leaving the acquirer vulnerable to risks presumed to be addressed and managed by the supplier [2].
3. **Geographical, social and cultural differences:** Reference to a law or a standard as a requirement in an agreement allows for misinterpretation by acquirer and supplier which results in a dispute or the service is provided in a location either unknown to or not permitted by the acquirer, leading to violations of acquirer's regulatory or compliance requirements.

2.3.6 Maturity Models

Maturity models have evolved to encompass not only organizational capabilities but also sectoral and national cybersecurity and resilience capacities [55]. The most widely recognized maturity model among researchers is the Capability Maturity Model (CMM), developed by the Software

Engineering Institute as a framework for describing the key elements of an effective software process and its evolution from an ad hoc and immature state to a mature and disciplined process. As Kohlegger[39] notes, a maturity model "represents phases of increasing quantitative or qualitative capability changes of a maturing element to assess its advantages concerning defined focus areas."

Maturity is the progression of a skill, process, or objective from an initial to a desired state, typically characterized by explicitly documented, managed, measurable, controlled, and continuously improved practices. Risk maturity refers to the level of sophistication and advancement in an organization's risk management processes and capabilities [53].

In the case of the CMM, processes are assessed on a scale of five maturity levels as Figure 2.4 shows. Apart from Level 1, each maturity level is composed of several key process areas, which are in turn organized into five common features:

- Commitment to perform
- Ability to perform
- Activities performed
- Monitoring implementation
- Verifying implementation

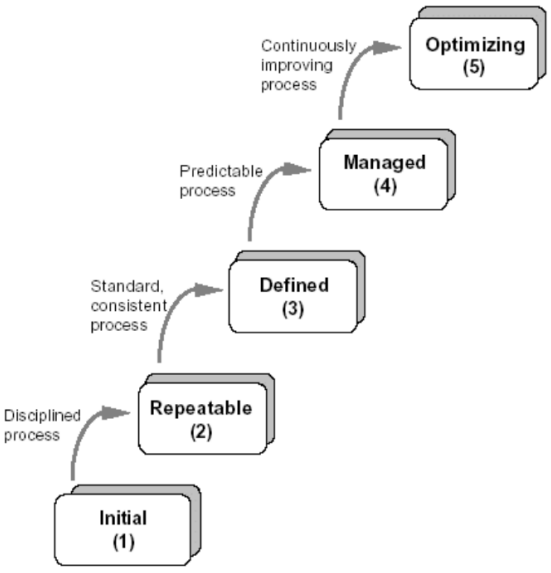

Figure 2.4: The five levels of software process maturity (extracted from [62])

Each level provides a layer in the foundation for continuous process improvement, with a set of goals that, when satisfied, stabilize a crucial component of the software process and increase the organization's process capability.

- **Level 1 – Initial:** Ad hoc, unpredictable processes, reliant on individual effort.

- **Level 2 – Repeatable:** Basic project management enables repeating past successes.
- **Level 3 – Defined:** Standardized, documented processes ensure organization-wide consistency.
- **Level 4 – Managed:** Quantitative metrics control processes for predictable performance.
- **Level 5 – Optimizing:** Continuous improvement through defect prevention and innovation.

2.4 Auditing

According to ISO 19011:2018 [29], auditing is a systematic, impartial, and objective activity carried out to determine whether a management system complies with specified requirements such as policies, standards, or legal obligations. The standard promotes a disciplined methodology built on key principles, including:

- **Integrity:** Auditors must act ethically, honestly, and impartially, avoiding undue influence on their judgment.
- **Fair presentation:** Audit results should be reported truthfully, accurately, and completely, including any obstacles or disagreements.
- **Due professional care:** Auditors should work diligently, using sound judgment that reflects the trust placed in them.
- **Confidentiality:** Information obtained during audits must be protected and not misused for personal gain or harm.
- **Independence:** Auditors should remain objective, free from bias or conflicts, and independent from the activities they audit.
- **Evidence-based Approach:** – Conclusions should rely on verifiable evidence, often gathered through appropriate sampling.
- **Risk Based Approach:** Audits should focus on areas of greatest risk and opportunity to meet programmed objectives.

The central aim is to obtain reliable, verifiable information that enables organizations to evaluate both compliance and performance, while also pinpointing opportunities for improvement. In contrast to informal reviews, audits provide a consistent and trustworthy mechanism for understanding how well internal controls function, how effectively processes are executed, and how closely the system aligns with predominant strategic objectives.

Audits serve as a structured means of examining supplier reliability, regulatory compliance, and process maturity. By applying a risk-based approach, organizations can focus resources on

the most sensitive areas of their supply chain, such as high-risk suppliers, critical outsourced operations, or sites under regulatory or geopolitical consideration.

They also enable objective benchmarking of supplier practices, verification of corrective actions, and evaluation of readiness for potential disruptions. This targeted assessment helps organizations identify weaknesses, implement tailored improvements, and strengthen the overall resilience of their supply networks.

An additional benefit lies in promoting transparency between organizations and suppliers. Because operational data can be sensitive, suppliers may be reluctant to share it openly. The auditing process addresses this by providing a formal, mutually agreed framework that safeguards confidentiality [23]. The standard[29] specifically emphasizes professional handling of sensitive information, which reassures suppliers and encourages constructive, trust-based collaboration.

Audits may be conducted at 3 different levels:

- **1st party audit:** Internal evaluation conducted by the organization itself
- **2nd party audit:** Assessment performed by a customer, external provider, or other interested party
- **3rd party audit:** Independent certification, accreditation, or regulatory/statutory audit

2.4.1 Auditing Programme

An audit programme should be developed, potentially covering one or multiple management system standards or other requirements, conducted individually or as a combined audit. Its scope should reflect the auditee's size, nature, operational complexity, associated risks and opportunities, and the maturity level of the management system(s) being audited.

When key functions are outsourced or managed by other organizations, especially across multiple sites or countries, special care must be taken to identify where major decisions are made and who forms the system's top management. Audit programme design, planning, and validation should reflect these complexities.

For smaller or less complex organizations, the audit programme can be scaled accordingly. To understand the auditee's context, the programme should consider:

- organizational objectives;
- relevant internal and external factors;
- needs and expectations of interested parties;
- information security and confidentiality requirements.

Audit resources and methods should be prioritized for areas of the management system with higher inherent risk and lower performance levels [59]. The audit programme should be overseen by competent personnel and contain the necessary information and resources to ensure audits are carried out effectively and efficiently within defined timeframes. This information should include:

- the objectives of the audit programme;
- risks and opportunities related to the audit programme, along with actions to address them;
- the scope of each audit, including its extent, boundaries, and locations;
- the audit schedule, covering number, duration, and frequency;
- the type of audit, such as internal or external;
- applicable audit criteria;
- the audit methods to be used;
- the criteria for selecting members of the audit team;
- relevant documented information.

Figure 2.5 demonstrates the process flow for the management of an audit programme:

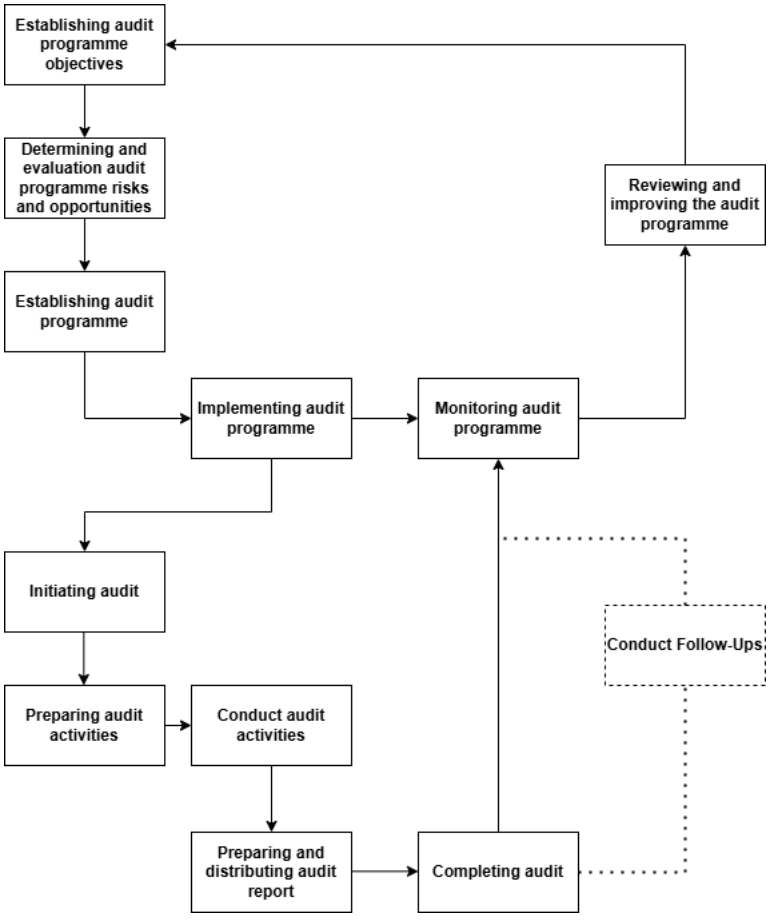

Figure 2.5: Process flow for the management of an audit programme (extracted from ISO/IEC 19011:2018[29])

Chapter 3

Related Work

This chapter examines key works related to the work, emphasizing the critical need for continuous management in supply chain risk. It provides an analysis of the current state of the art, explores the advantages and challenges associated with alignment, visibility, and trustworthiness in risk management, explores the concept of risk compensation method, and suggests a potential framework for evaluating the supply chain risk management process (risk maturity).

3.1 Identifying Key Challenges

According to ISO/IEC27036[32], to effectively manage information security in supplier relationships across the ICT supply chain, acquirers should implement a framework containing the following standardized, organization-wide processes for acquiring products and services:

1. Define information security and compliance requirements to ensure the secure exchange or sharing of information and systems.

2. Evaluate and monitor information security risks associated with the supply chain before acquisition.

3. Develop a process for negotiating or renegotiating ICT supply chain agreements. These agreements should incorporate information security and compliance requirements, including provisions for audit rights and restrictions on upstream suppliers across multiple supply chain tiers.

4. Continuously monitor and report on supplier performance within the ICT supply chain to ensure adherence to information security and compliance requirements, particularly when supplier relationships change.

This framework should be designed with flexibility to support a variety of ICT supply chain agreements, tailored to the unique characteristics and risks associated with the specific product or service being acquired. It should be built upon the foundation established in ISO/IEC 27005[35]. According to the National Institute of Standards and Technology (NIST) on their last request

for information (RFI)[51] there's a pressing need to develop a cybersecurity framework that is accessible and practical for organizations of all sizes to understand and manage risks effectively [54]. This framework must be designed to allow incremental development, enabling organizations to build upon it while ensuring backward compatibility. It should align with international standards such as ISO/IEC and NIST, fostering consistency and compatibility across systems. Furthermore, the framework should maintain neutrality, serving both suppliers and acquirers, and be adaptable to various contexts.

Given the growing complexity of supply chains, it is crucial to establish key tiers within the chain and provide clear guidance on maturity models to enhance security practices [9]. Additionally, there is a strong need for improved guidance on inventory management across the supply chain, encompassing software, hardware, contracts, and their ongoing oversight .

3.2 Complexity in Supply Chains

As mentioned in the chapter 3.1, the complexity of supply chains arises from the interconnected flows of materials and information among different partners. In the past, these flows were organized in a linear sequence, moving from suppliers to the final customer. Today, modern technologies have transformed this structure. Information is no longer restricted to one-way, step-by-step movement; instead, it circulates dynamically and simultaneously, enabling real-time sharing and collaboration across all partners in the chain [64].

This shift provides greater visibility, coordination, and responsiveness. Partners can access key data such as inventory levels, demand forecasts, and production schedules, which supports smarter decisions and more efficient operations. While this simultaneous exchange of information adds new layers of complexity [50], it also creates opportunities for improved efficiency, flexibility, and overall performance when managed effectively.

To fully realize these benefits, supply chain partners need to adjust their processes and technologies while developing a comprehensive understanding of core business operations. The Supply Chain Operations Reference (SCOR) model provides a vital framework for modeling, assessing, and improving supply chain performance [13]. As illustrated in figure 3.1, this model has evolved from a linear to a circular approach.

3.2.1 SCOR Model

The Supply Chain Operations Reference (SCOR) model is a process reference framework (demonstrated in figure 3.2) created by the Supply Chain Council in the 1990s to provide a standardized method for describing, analyzing, and improving supply chains [56]. It integrates processes, performance metrics, best practices, and skills into a unified structure, establishing a shared language that promotes synchronization among stakeholders and supports effective modeling of logistics systems [26, 19]. At its foundation, SCOR is structured around five core management processes that span the entire supply chain:

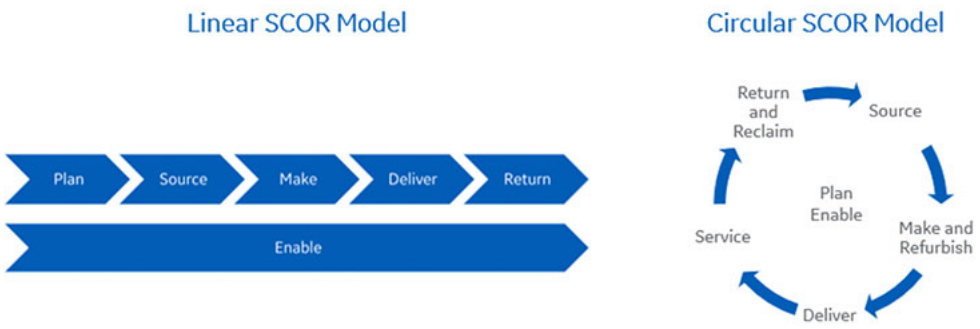

Figure 3.1: SCOR Model evolution from Association for Supply Chain Management [27]

- **Planning**: involves gathering customer requirements, collecting information on available resources, and balancing requirements and resources to determine planned capabilities and identify any resource gaps.
- **Sourcing**: encompasses activities related to the ordering and receipt of goods and services from suppliers.
- **Making**: covers activities involved in the conversion of materials or the creation of content for services.
- **Delivering**: includes activities associated with the creation, maintenance, and fulfillment of customer orders.
- **Returning**: covers activities related to the reverse flow of goods from the customer, including product returns and reverse logistics.

By mapping operations into specific categories, organizations are able to diagnose flows between suppliers and customers more effectively. This categorization also makes it possible to apply standardized metrics that assess performance consistently and to establish shared strategic objectives [8].

Building on this foundation, the SCOR model serves not only as a descriptive framework but also as a strategic enabler for supply chain transformation. Its standardized performance attributes allow firms to benchmark themselves against industry peers and define measurable targets for improvement [4]. These attributes include:

- Reliability
- Responsiveness
- Agility
- Cost
- Asset efficiency

Research further emphasizes that the SCOR model is valuable beyond diagnosing inefficiencies. It also plays a significant role in supporting engineering projects, particularly when it is integrated with information systems that enhance supply chain visibility and coordination [8].

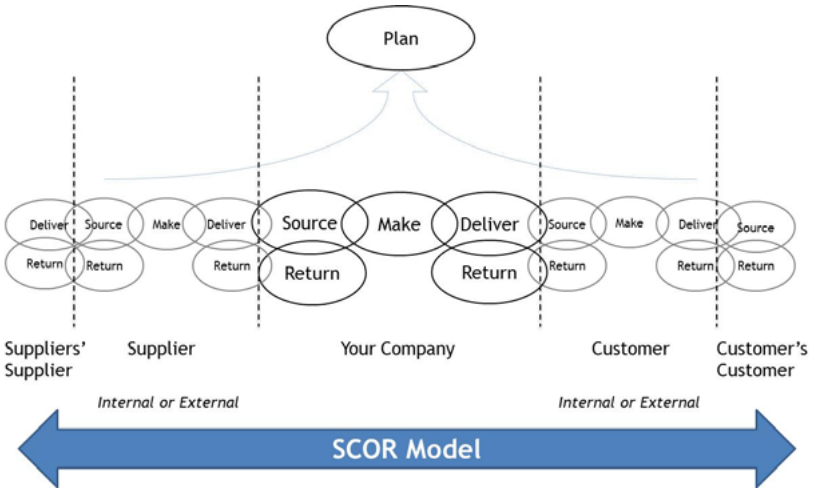

Figure 3.2: SCOR Model (extracted from [1])

3.3 Acquisition in the Supply Chain

Organizations source hardware, software, and services from various suppliers, who themselves may rely on other providers for components. The information security risks inherent in these complex and layered supply chains can be addressed through robust risk management practices and the cultivation of trusted relationships. This approach enhances trustworthiness, and transparency across the hardware, software, and services supply chain [36, 40].

3.3.1 Acquirer and Supplier Relationship Types

Acquirers and suppliers of hardware, software, and services may engage with numerous entities through various supply chain relationships, including but not limited to [37]:

- information or operational system management support where systems are owned by the acquirer and managed by the supplier;
- information or operational systems or services providers where systems or resources are owned and managed by the supplier;
- product development, design, engineering, etc. where the supplier provides all or part of the service associated with creating hardware and software;
- commercial-off-the-shelf product suppliers;
- open source product suppliers and distributors.

When acquirers grant suppliers access to their information and systems, they increase their reliance on the provided hardware, software, and services. This heightened dependency amplifies risk, necessitating a higher degree of trust in suppliers. For instance, acquiring management support for information or operational systems often carries greater risk than obtaining open-source

or commercial off-the-shelf products. From the supplier's perspective, any compromise to the acquirer's information can damage the supplier's reputation and erode trust with the affected acquirer [57].

3.3.2 Acquisition Process

The goal of the acquisition process is to secure a product or service that meets the acquirer's specific requirements. To effectively manage supply chain risks associated with hardware, software, and services, acquirers should incorporate the following steps into the acquisition process according to ISO/IEC 27036-3 [32].

Preparing for the Acquisition

1. **Establishing a Strategy:** The acquisition process begins with defining a strategy that outlines how the acquisition will be conducted. This includes:

    - Creating sourcing strategies based on the organization's risk tolerance related to hardware, software, and services supply chain risks.
    - Specifying a baseline set of information security requirements that will apply to all supplier relationships.

2. **Tailoring Baseline Security Requirements:** The baseline information security requirements should be customized for specific supplier relationships to prepare a comprehensive request for product or service supply. These tailored requirements should include:

    - Establishing information security requirements for suppliers, covering regulatory, technical, and operational aspects such as chain of custody, transparency, and incident reporting across the supply chain.
    - Requiring suppliers to manage their own suppliers in the supply chain as appropriate.
    - Defining requirements for suppliers to provide credible evidence of compliance with security standards.
    - Mandating suppliers of critical elements to demonstrate capabilities for addressing emerging vulnerabilities and responding to incidents effectively.
    - Identifying intellectual property ownership and responsibility for elements like software code, data, manufacturing environments, designs, and proprietary processes.
    - Defining physical security expectations, such as requiring suppliers to use secure data centers that meet the acquirer's standards.
    - Requiring suppliers to specify the expected lifespan of supplied elements to assist in long-term planning.
    - Demonstrating robust software supply chain practices.

- Establishing requirements for auditing suppliers' information systems and monitoring their work processes where applicable.
- Communicating the acquirer's requirements throughout the supply chain, ensuring alignment with upstream suppliers.

Advertising the Acquisition and Selecting Suppliers

1. **Communicating the Request:** The acquirer must communicate the product or service requirements to identified suppliers. No specific actions related to hardware, software, and services supply chain risks are required during this step.
2. **Supplier Selection:** Suppliers should be selected based on their ability to meet the specified requirements, including supply chain-related needs. The selection process involves:
   - Using established evaluation methods and criteria, such as ISO/IEC 15408 repositories or ISMS certification, to assess conformance.
   - Considering suppliers' past performance, including their personnel policies, procedures, and information security practices, as part of the evaluation process.

Initiating Agreement

1. **Negotiating with Suppliers:** The acquirer should negotiate agreements with selected suppliers, ensuring that all agreed-upon hardware, software, and services supply chain requirements are clearly stipulated in the contracts.
2. **Commencing the Agreement** A plan should be established to ensure the integrity of acquired products and components, focusing on the hardware, software, and services supply chain.

Monitoring the Agreement

1. **Assess the execution of the agreement:** Monitoring the agreement involves verifying compliance and maintaining oversight through:
   - Verification procedures and criteria for delivered products and services.
   - Auditing suppliers' information systems, as applicable.
   - Monitoring suppliers' design and delivery practices as well as their work products.
2. **Providing Support and Addressing Issues:** The acquirer must report any information security weaknesses or vulnerabilities discovered during the use of supplied hardware, software, or services. Timely resolution of issues and data sharing with suppliers is critical.
3. **Evaluating Supplier Performance:** Suppliers should be evaluated for their ability to meet the specified supply chain requirements throughout the agreement.

Accepting the Product or Service

1. **Verifying Compliance:** The delivered product or service must comply with the terms of the agreement. No additional actions specific to the hardware, software, and services supply chain are required during this phase.

2. **Closing the Agreement:** Once compliance is confirmed, payment or other agreed-upon considerations should be made to the supplier, marking the close of the agreement. No specific activities related to the supply chain are necessary at this stage.

3.3.3 Supply Process

The supply process aims to deliver a product or service that fulfills the acquirer's agreed-upon requirements. To effectively manage and demonstrate control over supply chain risks related to hardware, software, and services, suppliers should incorporate the following steps into their supply process according to ISO/IEC 27036-3 [37].

Identifying Opportunities

1. **Determining Acquirer Needs:** The first step involves identifying whether an acquirer exists and determining their need for a product or service. This assessment should establish if the acquirer represents an organization or group requiring the product or service. No specific actions related to the hardware, software, and services supply chain are required at this stage.

Responding to a Tender

1. **Evaluating the Request:** Evaluate the request for the supply of a product or service to determine its feasibility and develop an appropriate response. This includes specifying a baseline set of information security requirements applicable to all acquirers, with the flexibility to tailor these requirements as necessary.

2. **Preparing the Response:** Prepare a response that addresses the solicitation and demonstrates the supplier's ability to meet the acquirer's information security requirements. These requirements include:

    - Hardware, software, and services-related regulatory compliance.
    - Chain of custody, transparency, and visibility.
    - Sharing information on supply chain-related incidents.
    - Rules for component disposal or retention of elements like data, components, or intellectual property.

Initiating an Agreement

1. **Negotiating with the Acquirer:** Negotiate the agreement terms with the acquirer. No actions specific to the hardware, software, and services supply chain are necessary at this point.

2. **Commencing the Agreement:** Once an agreement is reached, establish and maintain plans to ensure:

    - The integrity of the included and delivered software and hardware products and components.
    - The protection of intellectual property rights, covering data, designs, processes, and development environments.

Executing the Agreement

1. **Implementing the Agreement:** The agreement should be executed following the supplier's established project plans. This phase does not require specific activities related to the hardware, software, and services supply chain.

2. **Assessing Execution:** Monitor the execution of the agreement as outlined. No additional actions specific to the supply chain are needed at this stage.

Delivering and Supporting the Product or Service

1. **Delivering in Accordance with Criteria:** The product or service must be delivered as per the agreement's specifications. This step does not involve specific activities related to the hardware, software, and services supply chain.

2. **Supporting the Delivered Product or Service:** Provide assistance to the acquirer in supporting the delivered product or service. Key activities include:

    - Responding to inquiries about ongoing security obligations, such as audits.
    - Providing support for incident response queries.

3. **Accepting Payment or Consideration:** Acknowledge receipt of payment or other agreed consideration for the delivered product or service. This phase does not require specific actions related to the supply chain.

Closing the Agreement

1. **Transferring Responsibility:** Conclude the agreement by transferring responsibility for the product or service to the acquirer or another designated party. No additional activities specific to the hardware, software, and services supply chain are required.

2. **Maintaining Security Measures:** Ensure all agreed security measures remain in effect or are properly terminated upon closure of the agreement.

3.3.4 Supplier Size

As illustrated in Figure 3.3 from a Eurostat study[15], SMEs account for approximately 99% of all businesses and employ an increasing number of people. Notably, around 94% of these enterprises operate independently, meaning they are neither controlled by another company nor do they control other enterprises. Consequently, special attention should be given to supply chain cybersecurity in the context of SMEs.

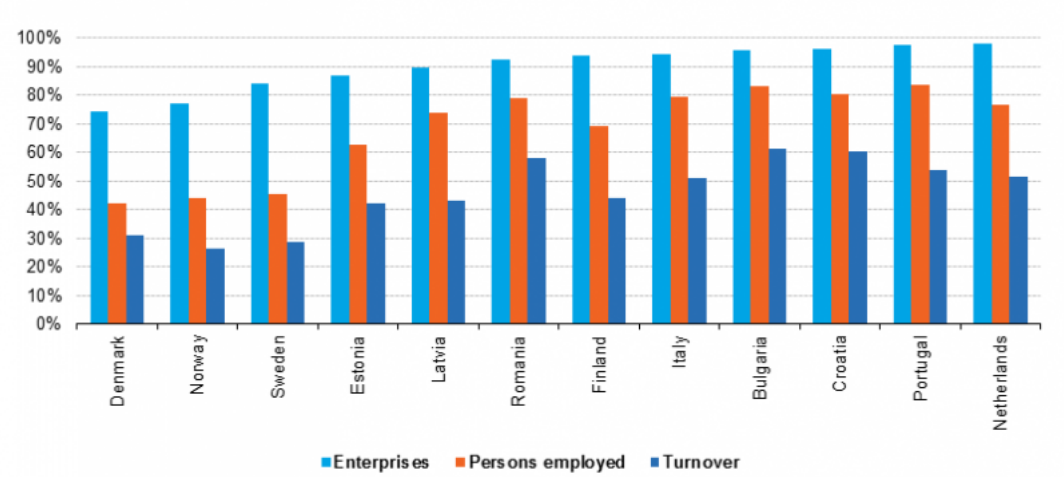

Figure 3.3: Number of enterprises, persons employed and turnover, independent enterprises share of all enterprises with fewer than 250 persons (extracted from [15])

The weakest link in a company's cybersecurity framework often lies within its supply chain, with particular attention focused on the role of small enterprises (SME), defined as companies with 250 or fewer employees and possessing either an annual turnover not exceeding €50 million or a balance sheet total not exceeding €43 million. These smaller entities, integral to the supply chain, face heightened susceptibility to cybersecurity threats. Targeted due to their unpredictable access to critical information relative to their size, they typically have weaker cybersecurity defenses owed to limited resources and capital. However, their attack surface and visibility are also dramatically smaller.

SME suppliers are often centered around distinctive and valuable capabilities, enabling them to transition smoothly across industries, customers, and supply chains. When required to enhance their performance in a specific area, such as cybersecurity, they typically respond in one of three ways: compliance, decoupling, or delaying action [65]. Furthermore, Melnyk[45] noted that some SME suppliers, when confronted with government mandates to strengthen cybersecurity measures, chose to exit the supply chain altogether [24].

Despite these vulnerabilities, these firms play indispensable roles in the supply chain by producing unique products relied upon heavily by larger partners, rendering them challenging to

replace. Addressing the cybersecurity concerns of these enterprise suppliers presents a unique challenge, given their limited understanding, resources, and expertise in implementing advanced cybersecurity systems. Consequently, enforcing compliance may risk these businesses, often possessing unique and crucial capabilities, withdrawing from the supply chain. This predicament raises an intriguing dilemma: finding ways to encourage these suppliers to make essential investments while ensuring their sustained participation in the supply chain [17].

3.4 Facing the Challenges

In addition to the challenges inherent in risk management, two critical issues that are consistently observed across supply chains are the lack of alignment between stakeholders and limited transparency in operational processes. To address these shortcomings, this work[52] explores two complementary mechanisms: a risk compensation system designed to encourage alignment and a more structured auditing framework to strengthen transparency.

3.4.1 Alignment

Alignment is a critical factor in achieving high cybersecurity capacity within the supply chain, especially in multi-tier supply chains. It refers to the extent to which the actors in a supply chain accept a common vision or objective and work together to achieve it, encompassing suppliers across each tier [17], this is demonstrated in figure 3.5.

According to a study presented in [17] there are two dimensions of alignment:

- Inter-organizational alignment (Horizontal lines in figure 3.4): the extent to which supply chain partners share a common vision and collaborate, recognizing their interdependence..
- Organizational alignment (Vertical lines in figure 3.4): the extent to which different levels within an organization agree on the importance of cybersecurity and act in support of it..

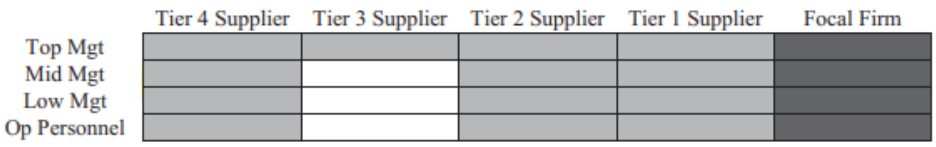

Figure 3.4: The challenge of achieving high cybersecurity capacity within a simple supply chain (extracted from [17])

This approach shows that supply chain cybersecurity needs to be seen as a whole-system effort. It's not just about technology but also about people's behaviour and how organizations work together. A lack of alignment can lead to fragmentation across different parts of the supply chain, resulting in concealed vulnerabilities that may be exploited by malicious actors. Accordingly, alignment is critical to ensure that all stakeholders, including lower-tier suppliers, collaborate in implementing robust cybersecurity measures and safeguarding the chain against potential threats.

Figure 3.5: The vision of alignment[47]

3.4.2 Transparency/Visibility

Transparency refers to the degree to which information is effectively shared among integrated partners, achieved through the seamless exchange of both internal and external data. Improved transparency in supply and demand conditions helps mitigate risks and supports agile production systems, enabling faster and more informed decision-making [43]. Prior research indicates that integration enhances coordination and collaboration across various organizational functions and supply chain partners, promoting the efficient flow of information and resources [20].

The resilience of partners and suppliers is a growing concern for companies. Resilience, in this context, means the ability of entities to withstand and adapt to challenges, particularly influencing their organizations future approach to cybersecurity. A significant majority expressed concern about their partners and suppliers' robustness, with nearly 58% of companies in the latest study by Enisa[44] expressing worry about their lower resilience compared to their own organizations.

Understanding the extended network of suppliers, including their own suppliers and contractors, is essential for improving visibility across multiple tiers of the supply chain [61]. This enhanced transparency is vital for fostering trust between vendors and buyers, enabling effective risk identification, and promoting the timely implementation of risk mitigation strategies [63].

Achieving transparency in supply chains faces numerous challenges for several reasons. Suppliers often view information about their supplier base as confidential and may resist sharing it, fearing that disclosing such details could lead to redundancy or replacement [38]. Additionally, the dynamic nature of supply chain relationships, where new suppliers frequently replace existing ones, further complicates the ability to maintain a comprehensive understanding of supply chain partners [17].

3.4.3 Risk Compensation

Risk compensation demonstrates the dynamic relationship between perceived risk and individual behavior [11]. This concept suggests that people may adjust their decision-making based on the level of risk communicated by the organization. Consequently, when the perceived risk is low, individuals may engage in riskier behavior, whereas enhanced risk perceptions can lead to more cautious decisions. Riskier behavior increases the likelihood of a disruption, an unexpected and

potentially adverse event that can significantly impact the normal flow or functioning of a process or system [5]. Such disruptions can introduce unforeseen challenges into the chain, necessitating adaptations and solutions.

Recognizing the implications of risk compensation is vital for organizations seeking to enhance their risk mitigation strategies. It highlights the importance of effective communication as a cornerstone in SCRM. Companies must be mindful of the potential for risk compensation in decision-making processes, prompting them to tailor their risk management strategies.

In a broader context, risk compensation illustrates the proactive nature of risk management, emphasizing the importance of anticipating and addressing potential issues before they arise. Despite challenges in gaining attention for preventive measures, adopting risk compensation strategies becomes a proactive investment in strengthening organizations against unforeseen events.

3.5 State of the Art Analysis

Supply chains are vulnerable to numerous risks that can significantly affect organizational performance and customer satisfaction. Therefore, achieving a high level of risk maturity is critical for ensuring resilience, optimizing performance, and enhancing cost efficiency. Organizations with well-developed risk management frameworks can navigate uncertainties and disruptions with agility and confidence. They excel in identifying, assessing, mitigating, and monitoring risks effectively [16]. Moreover, a mature approach to risk management boosts stakeholder trust, ensures compliance with industry standards and regulations, and provides a strategic edge in the marketplace. Consequently, cultivating risk maturity in supply chains is vital for maintaining operational continuity, reducing disruptions, and achieving a competitive advantage in the global business arena [21].

To this end, two models will be evaluated: one specifically designed for supply chain risk management, and another focused on risk management maturity. The latter constitutes a generic framework that is applicable across diverse organizational domains, thereby providing a broader perspective on risk management practices.

3.5.1 Risk Management Model

The Supply Chain Risk Management Model of NATF[47] is designed to offer a streamlined, efficient, and industry-recognized method for organizations to assess the security practices of their suppliers. This model, when widely adopted, aims to ease the burden on suppliers, enhance the quality and quantity of information available to organizations, and strengthen supply chain security. The tools included in the model, along with the supporting services provided by solution providers, offer essential insights for organizations to consider during risk assessments of potential product and service suppliers.

The five-step model offers a robust framework for identifying, assessing, and mitigating supply chain risks. It accommodates the inclusion of suppliers and solution providers based on the specific

needs of each organization and allows flexibility in how each entity implements it. The model addresses supply chain risk management through five lifecycle phases (demonstrated in figure 3.7:

Figure 3.6: Supply Chain Security Risk Assessment lifecycle (extracted from [47])

Each phase of the life-cycle takes the following actions:

1. **Gather information:** Organizations start by collecting supplier data using tools such as:
   - **The NATF criteria:** A set of best-practice benchmarks that can be applied to request details from a supplier or to evaluate their security posture.
   - **The NATF Questionnaire:** A more detailed survey designed to capture specific insights into the supplier's supply chain risk management performance.
2. **Review information and address risks:** After collection, the information is analyzed to determine:
   - The extent to which the supplier's practices align with the criteria or questionnaire responses, and whether any gaps indicate risk.
   - The required level of confidence or verification in the supplier's statements.
   - Whether identified risks can be mitigated, accepted, or need escalation.
3. **Conduct a risk assessment:**
   - Apply a clear and consistent methodology for assessing supplier risks.
   - Document the results to support traceability and future decisions.
4. **Make purchasing decisions:**
   - Integrate the outcomes of supplier risk assessments into a cross-functional purchasing process.
   - Weigh risk appetite and other organizational factors in the selection.
   - Ensure that mitigation measures can be supported and enforced through contract terms.
5. **Apply controls and monitor continuously:** Once a supplier is chosen, the organization should:
   - Track risks and mitigation measures throughout the lifecycle of the product or service.
   - Monitor the supplier for significant changes (organizational shifts, supply chain modifications, or security breaches) that could affect the agreement.

3.5.2 Maturity Model

A maturity model consists of a sequence of maturity levels for a class of objects (usually organizations or processes) [21, 41]. It represents an anticipated, desired, or typical evolution path of these objects shaped as discrete stages. The RMMM from proença[53] aims to enhance the impact of risk management on an organization's business value. As organizations progress from lower to higher maturity levels, this impact grows, as illustrated in Figure 3.7 [3].

At lower levels, the absence of formal procedures and policies often results in poor-quality risk management, leaving organizations vulnerable without even being aware of the risks. Advancing to higher levels mitigates this risk by establishing, defining, documenting, and evaluating comprehensive policies and procedures. At the highest maturity level (Level 5), risk management becomes a source of competitive advantage, fully integrated into the organization's strategic framework. The figure also highlights the focus of risk management at each level and the outcomes associated with each stage [53].

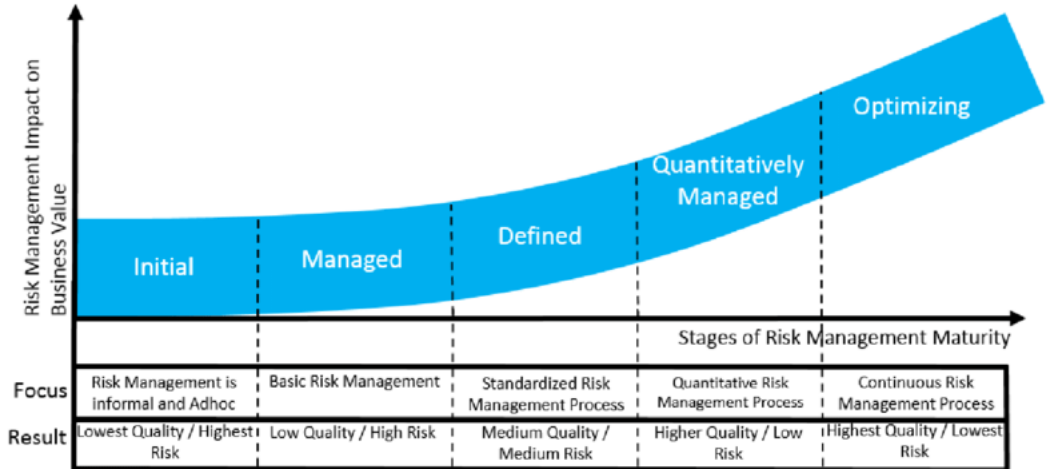

Figure 3.7: RMM Curve according to Proença[53]

In addition to the standard maturity levels (1–5), a Level 0 has been introduced, representing organizations that do not engage in any risk management processes or tasks. However, Level 0 is not explicitly included within the RM Maturity Model framework. Thus, the model comprises the following maturity levels:

- **level 0:** Non-existent risk management
- **level 1:** Initial risk management
- **level 2:** Managed risk management
- **level 3:** Defined risk management
- **level 4:** Quantitatively risk management
- **level 5:** Optimizing risk management

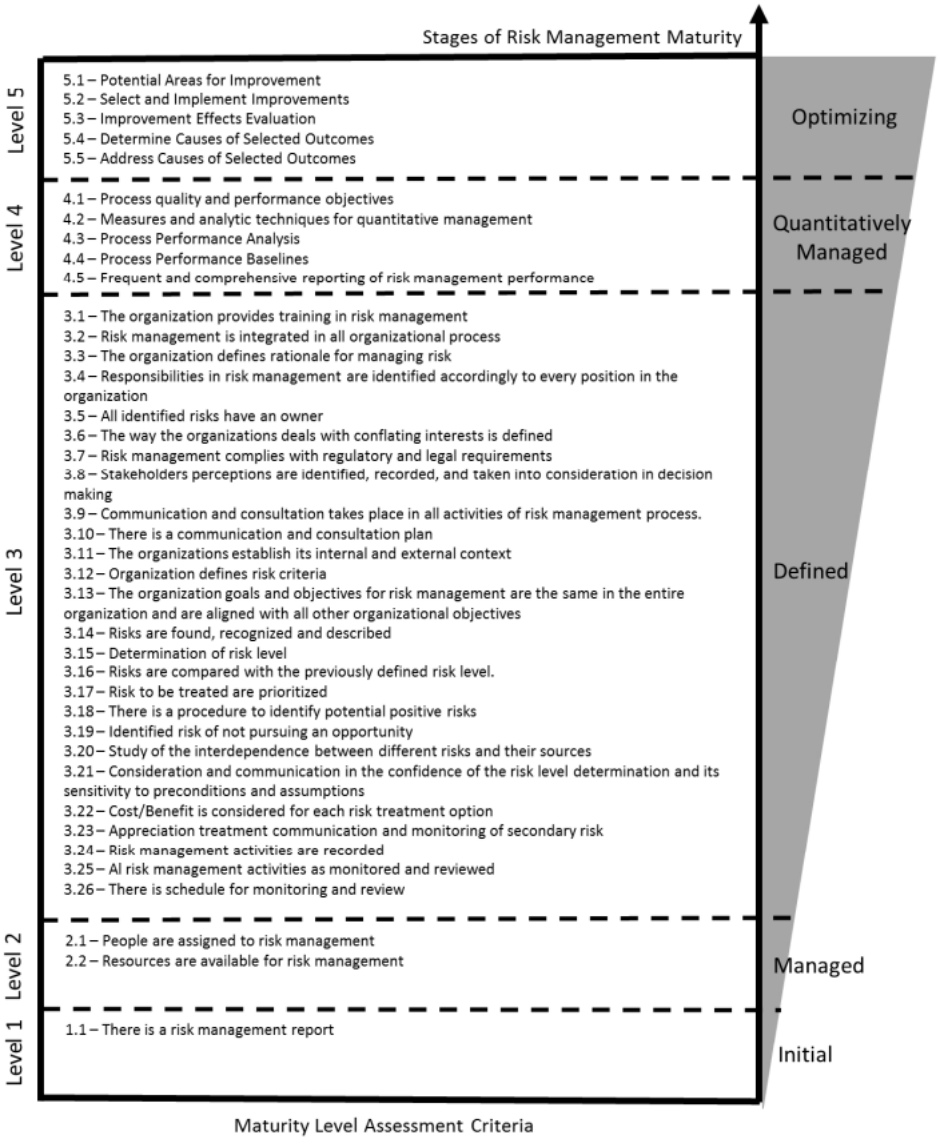

Figure 3.8: RM Maturity Model according to Proença[53]

Progression through the maturity levels follows a staged approach, requiring compliance with all criteria of the preceding level before advancing. This progression leads to an RM process that becomes progressively more managed, defined, and optimized over time [9].

To mature from level 0 to level 1, an organization must recognize the necessity of a risk management (RM) process as a vital organizational function. At level 1 (Initial), basic RM tasks are conducted to ensure some degree of risk management, though these efforts are often ad hoc, chaotic, and reactive rather than preventive. The organization lacks a stable environment to implement a formal RM process, with outcomes largely dependent on individual competence rather than a consistent methodology.

At level 2 (Managed), the organization begins planning and executing RM activities aligned with an established risk management policy involving stakeholders. While efforts are made to

formalize processes, practices often rely on repetitive actions from past successes rather than structured methods. Responsibilities are assigned to qualified personnel with adequate resources, enabling some degree of repeatability. However, the lack of uniformity means RM practices vary significantly across departments.

By level 3 (Defined), the RM process is fully characterized, standardized, and supported by documented procedures, tools, and methods. This level establishes consistency across the organization, with a centralized and evolving approach to RM.

At level 4 (Quantitatively Managed), the organization employs quantitative and statistical techniques to manage, measure, and evaluate the RM process systematically. This data-driven approach enhances precision and decision-making.

Finally, at level 5 (Optimizing), the organization continuously refines the RM process based on insights gathered at previous levels. RM is deeply integrated into the organizational strategy, with a culture of innovation driving advancements. Organizations at this level contribute to the broader domain of RM through scientific and methodological innovations.

Chapter 4

Framework

This chapter introduces the Supply Chain Cybersecurity Risk Management Maturity Model, which forms the foundational theoretical framework for this study. The model has three primary components:

1. SCOR Model Implementation
2. Supply Chain Risk Management Process Framework with usage of Maturity Seals
3. Auditing and Compliance Process

These three components collectively enable the assessment of maturity levels across individual assets within the supply chain and establish a basis for the continuous improvement of overall maturity over time.

4.1 Objectives

The proposed model incorporates information security requirements into supply chain relationships, including suppliers, subcontractors, and partners, to ensure compliance with established standards. It outlines clear guidelines for educating and informing supply chain members about their responsibilities, as well as the policies and procedures for accessing and managing information assets. This approach protects the organization's internal network and information systems against misuse, theft, fraud, or malicious activities, promoting trust and transparency among supply chain participants. Designed with flexibility in mind, the model allows for the addition or removal of steps, enabling organizations to alter it to their specific needs at any time.

The proposed model will be developed on the basis of established frameworks however, modifications will be introduced to adapt them to SCCRMM. The resulting framework seeks to provide a comprehensive approach for identifying, analyzing, and evaluating potential risks within the supply chain and their interdependencies. In doing so, it aims to establish a standardized maturity model, addressing a gap in existing frameworks that do not sufficiently capture the complexities of supply chain cybersecurity risk management.

It begins by assessing a new business need and determining whether supplier involvement is necessary. The risk assessment process follows with the aim of empowering risk owners to prioritize risks based on treatment strategies. This empowerment aims to enhance the overall risk maturity of the supply chain, fostering a proactive approach to risk management.

4.2 Scope

This model applies to all information assets managed by the organization's information security management system, including the related storage, transferring, and processing resources. It is designed for third parties, such as service providers, suppliers, partners, and others, who have a legal relationship with the organization and are within the scope of the overall information security system. This includes those who have access to, the right to use, or control over the organization's information assets and/or associated resources.

This model is designed to provide the supply chain with a structured and practical process, focusing on the aspects:

- Support in decision-making during the selection process of supplier to be contracted;
- Inform stakeholders about existing contractual relationships and concerns identified from an information security perspective;
- Define a supply chain method of evaluation compliance while safeguarding owners interests;
- Promote trust between suppliers;
- Promote the need for transparency between third parties and contractual relationships;
- Assist in defining a clear plan to enhance the risk maturity of the chain through the risk management process.

4.3 Implementation Framework

To build a comprehensive framework, insights from the literature review were integrated with an analysis of the relevant environment, resulting in a practical reference for practitioners.

In order to incorporate all findings into a single holistic framework, the process is organized into three distinct phases: the pre-implementation phase (A), the implementation phase (B), and the continuous improvement phase (C).

The pre-implementation phase (Phase A) focuses on establishing the right conditions for the successful adoption of initiatives. Its objective is to address all critical success factors and implementation requirements, ensuring that the most suitable methods and techniques are selected based on the asset targeted for improvement. This careful alignment maximizes the potential benefits during implementation.

The implementation phase (Phase B) begins when the strategy is put into practice. This stage involves translating plans into actionable steps, with further details provided in the following subsection.

The improvement phase covers all activities that support ongoing improvement and the advancement of supply chain risk maturity. It involves evaluating maturity levels by comparing actual performance against defined goals, enabling the identification of areas for enhancement.

The framework process is illustrated in Figure 4.1. It begins with the Process Discovery (Part of the Pre-Implemantion Phase), starting with data collection. At this stage, stakeholders are identified, and the asset under evaluation is specified, with relevant information gathered, such as potential disruption impacts, the current risk level, and expected downtime recovery time. Its status within the SCRMM is then assessed. These elements collectively compose the scope of the SCOR model, encompassing the establishment of evaluation metrics, the selection of processes for assessment, and the clarification of expected acquisition outcomes. This structured approach, guided by the SCOR model, supports an informed decision on whether to proceed with the acquisition, ensuring that advancement is based on defined maturity metrics and objectives.

The process then advances to the Implementation Phase, which encompasses Identification, Analysis, and Decision. In this phase, the requirements for acquisition are first established, followed by the initiation of the supplier search. Potential suppliers respond to the organization's request for tender, after which each supplier undergoes a structured evaluation. This evaluation, conducted during the analysis stage, defines the distribution of responsibilities, which may vary across suppliers. The supplier's maturity seal level is also considered, providing insight into their approach to risk management maturity. Based on these assessments, together with an evaluation of potential incident consequences related to the asset, a revised risk level is determined. This risk-informed assessment ultimately supports the decision-making stage, culminating in the formalization of a contract if the acquisition proceeds.

If the acquisition proceeds, a Maturity Assessment is conducted as part of the Improvement Phase. In this stage, the organization's maturity is reassessed in light of the acquisition's impact. Simultaneously, areas for improvement are identified, leading to the selection of new initiatives aimed at updating the scope of the SCOR model. This process generates revised evaluation metrics and guides continuous development until the desired level of supply chain risk management maturity is achieved.

The following sections provide a detailed examination of each component of the framework. The discussion above is therefore intended as a high-level overview, outlining the main processes before proceeding to their in-depth analysis.

4.4 Pre-Implementation Phase

The adoption of new techniques within a framework can influence the entire organization and therefore requires careful attention to stakeholders in order to limit resistance and strengthen participation. The first step is to build awareness and obtain support from stakeholders.

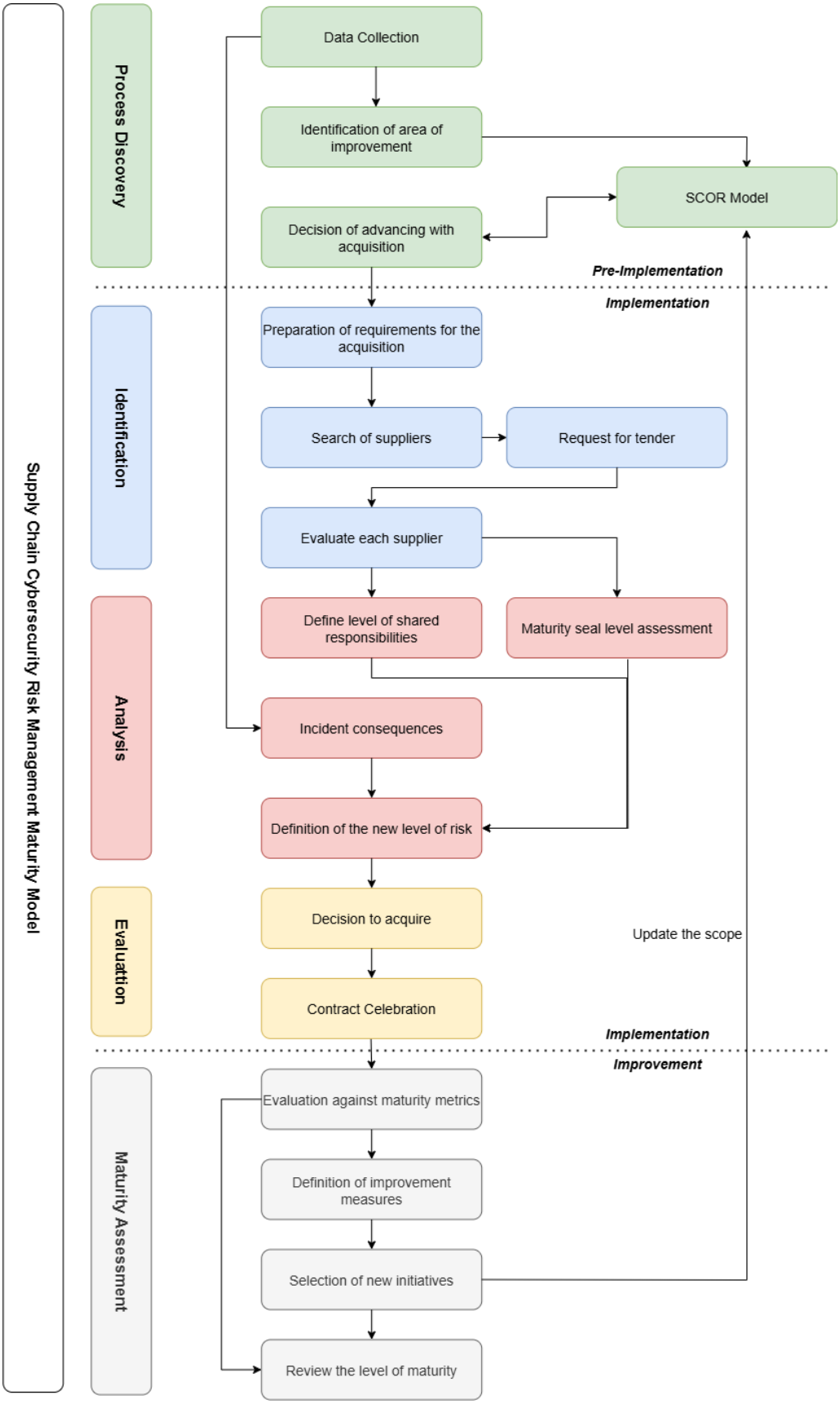

Figure 4.1: Framework Process Overview

4.4.1 Process Discovery

A thorough examination of the organization's supply chain is required at this stage, taking into account its capabilities, constraints, strengths, and vulnerabilities, with stakeholder engagement playing a pivotal role as their insights and support strongly influence the effectiveness of risk management initiatives, which in turn gives rise to key questions such as:

- Is the supply chain risk management sufficiently mature for this asset to address current and emerging risks, or are improvements needed to advance its level of maturity?
- Do we possess the resilience and momentum required to respond effectively to disruptions?
- Are our teams equipped with the necessary expertise to identify, evaluate, and mitigate risks, or should additional competencies be developed or acquired?
- Do we have the tools, resources, and technologies required to monitor risks and strengthen controls across all supply chain tiers?

Defining clear roles, ownership, responsibilities, and decision-making authorities is fundamental for the success of the process. The organization must also designate those responsible for executing and continuously monitoring the process, while actively engaging all relevant stakeholders. This decision may depend on factors such as the size and organizational structure of the company. Alignment across roles and governance mechanisms is critical to fostering cross-functional collaboration between business and IT units.

Table 4.1 provides a conceptual example of a communication strategy, structured to address the specific requirements of diverse stakeholders, and intended to be adapted in accordance with contextual needs.

The proposed changes presents benefits but demand considerable investments of time, funding, and resources (financial, operational, technical, and human). Recognizing and preparing for this long-term commitment is essential in this phase. Careful and diligent planning is critical, as these factors ultimately determine the success of achieving the intended objectives.

Prior to implementation, it is essential that all stakeholders are comprehensively informed and adequately educated regarding the planned initiatives and their objectives. Establishing effective communication channels to promote awareness and transparency, while simultaneously encouraging knowledge sharing, training, and collaboration, represents a critical foundation for successful execution. Equipped with enhanced understanding, stakeholders are more inclined to support innovation, demonstrate active engagement, and apply process mining solutions with greater effectiveness, for that we will use the SCOR Model.

For the purposes of this thesis, the discussion begins with an examination of the inherent complexities of supply chains. This is followed by an analysis of how these complexities have influenced the scope of cybersecurity standards, thereby reinforcing the relevance of the proposed framework. Subsequently, the SCOR model and its significance is introduced.

Stakeholder	Detail of Information	Reporting Cycle	Communication Scope
Consumers	High-level, simplified overview	Periodic (quarterly or when incidents occur)	Risk assessment results, key security priorities, impact on business objectives
Developers	Technical and detailed	Continuous (development cycles / when vulnerabilities are detected)	Technical requirements, vulnerability reports, mitigation procedures
IT/Cyber Leads	Balanced: mix of technical and managerial detail	Regular (monthly meetings or project phases)	Identified risks, proposed controls, alignment of risk treatment strategies
Evaluators	Detailed, evidence-based	At audit checkpoints or after risk assessment cycles	Compliance status, conformity reports, effectiveness of controls, audit findings
Management	Executive-level summaries with key metrics	Strategic reviews (biannual or annual)	Overall risk posture, major incidents, compliance with frameworks, investment needs

Table 4.1: Examples of stakeholder communication

4.4.2 Supply Chain Relationships

In Section 2.1.3, we outline security concepts and their relationships based on ISO/IEC 15048-1[28]. However, in the context of supply chain cybersecurity, a deeper analysis of these relationships is necessary. It is crucial to consider suppliers and their influence on vulnerabilities and threats to assets. Therefore, Figure 4.2 is designed to illustrate these interconnected relationships.

Assessing third parties that directly or indirectly influence a company's assets, whether related to information or personal data, is essential. Their involvement can span various stages, from software development and maintenance to compliance and auditing.

To address this, Figure 4.2 has been adapted to incorporate key concepts in the supply chain management process (it's worth nothing that while the concept "vulnerabilities" is added to the framework it should be seen as decomposition of the interactions between the controls and risk to further enhance a full comprehension on the depth that supply chain adds to the paradigm) with the following additions to the framework:

- **Suppliers (Third Parties):** Entities that provide goods, services, or raw materials to a company as part of the production or operational process.
- **Requirements:** The contractual obligations that should be imposed by the organization owners and that should be met by the suppliers regarding the management of assets
- **Vulnerabilities:** Can either be regarding the assets of suppliers or from a breach in contractual obligations.

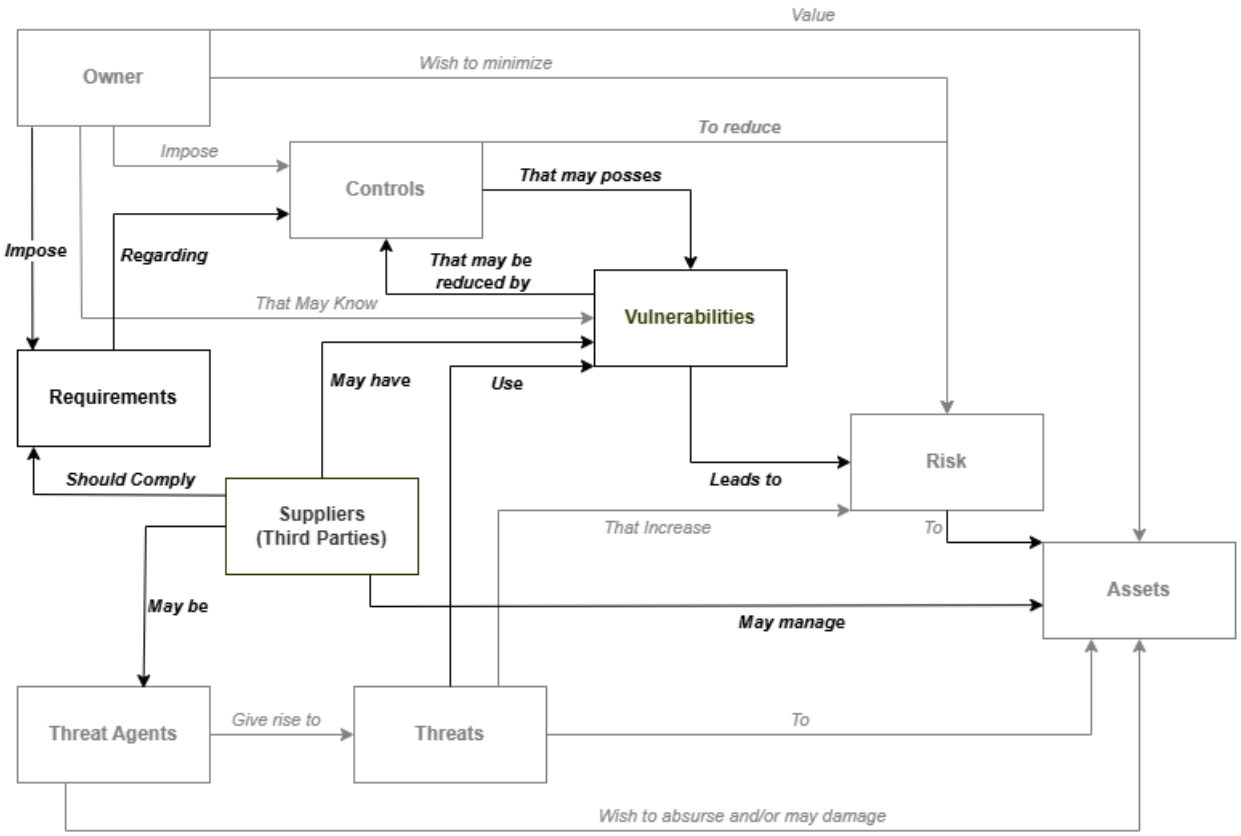

Figure 4.2: Supply chain security concepts and relationships (Adapted from ISO/IEC15048-1 [28])

4.4.3 SCOR Model

The SCOR model enables us to dissect the supply chain into ideal business processes and categories, facilitating a comprehensive cross-company analysis of all information, financial, and product flows within the chain. Consequently, based on our implementation phase, we can plan long-term, medium-term, and short-term while coordinating and comparing processes between suppliers, manufacturers, and customers, thereby increasing efficiency and effectiveness.

Implementing the SCOR Model's ideology empowers us to precisely define the scope of the process we seek to improve, and establish the metrics and performance measures that we will evaluate post-improvement. These pre-defined factors will serve as our basis of comparison moving forward. The aim is to advance the process to a higher level of maturity by leveraging new technologies. By reassessing performance metrics post-implementation, it becomes possible to evaluate improvements in the process's maturity level.

4.5 Implementation Phase

If the decision to advance with acquisition receives positive feedback from stakeholders, we can proceed with the Risk Identification , the initial step of the implementation phase. At this stage, a

comprehensive risk management process is carried out to evaluate the effectiveness of integrating a new acquisition into the overall chain.

Every project in the corporate portfolio must align with the organization's objectives and strategy. Making well-informed decisions and clearly defining business needs, purpose, scope, and objectives are crucial when deciding to initiate a supply chain risk assessment.

4.5.1 Risk Identification

The identification phase begins when the organization chooses to engage suppliers to meet its needs. Figure 4.3 illustrates the resulting activities from this decision, which will subsequently shape the next phase based on the selected requirements.

The company begins by compiling a provisional impact analysis on the asset by acquiring a third party. The decision to select a supplier is based on the volume required and overall cost considerations. Once the requirements are determined, the company prepares a request for tender.

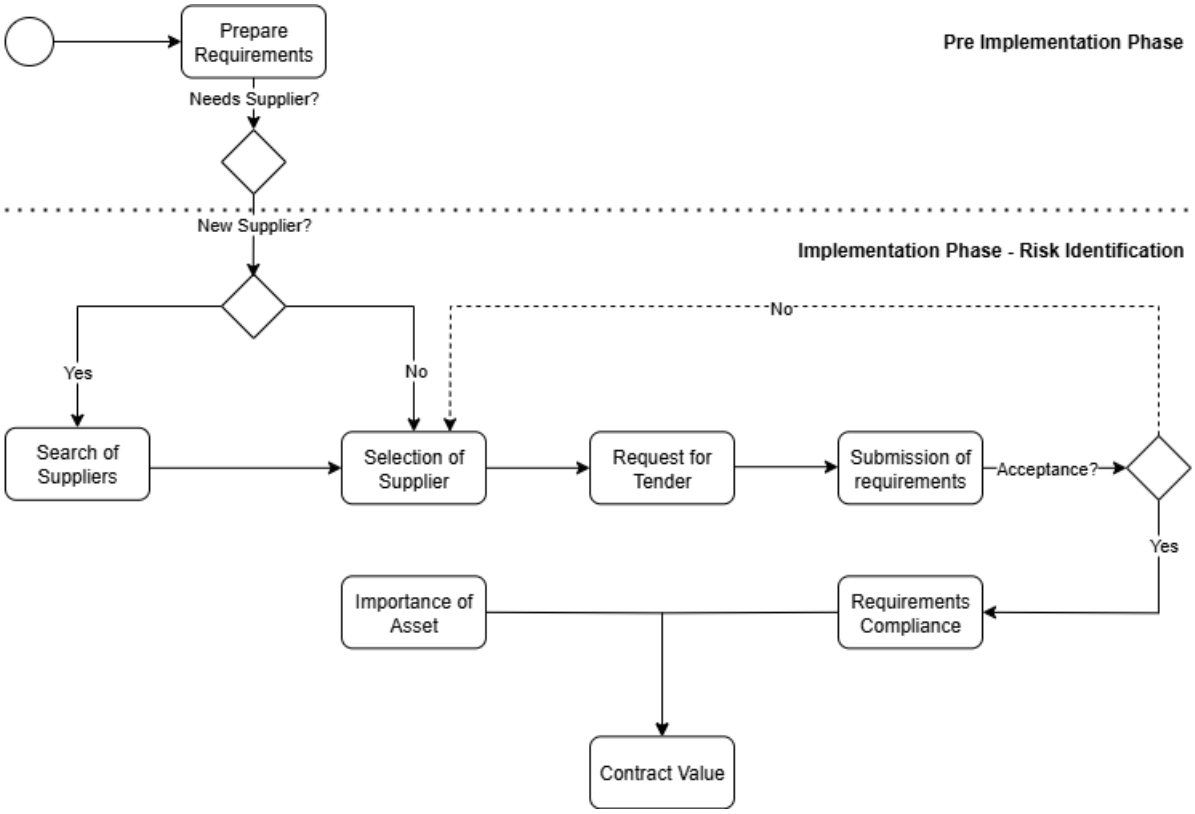

Figure 4.3: Identification of Acquisition process

Before initiating the identification process, it is essential to ensure that all relevant third parties and assets are properly identified and recorded. This process can begin in three scenarios:

- When evaluating potential new third parties for collaboration with the organization.
- When adding or modifying a contractual relationship with an existing third-party collaborator.

- When modifying a contractual relationship with, there is an addition of a tier 2 supplier that directly impacts the asset in question.

From a supply chain risk assessment point of view, formally documenting all related activities is crucial. This documentation facilitates a structured analysis and evaluation process, strengthening the overall risk maturity of the supply chain risk.

Regardless of the activity, supplier discovery is essential. This structured process involves systematically collecting and validating critical information about prospective or newly considered suppliers prior to granting approval for the provision of goods or services. Even when a supplier that initially generates interest is not selected, maintaining a record of it is important, as it facilitates the foundation for potential future collaborations involving other resources. Furthermore, it functions as a mechanism for the continuous and efficient monitoring of supplier status and performance.

After the organization has identified and selected a list of possible suppliers (those deemed suitable to provide the specific asset), it proceeds with a Request for Tender (RFT). In this step:

- A list of requirements is made that addresses all the criteria regarding the asset
- A formal invitation is made the selected suppliers to submit their proposals
- Evaluation of proposals and selection

After the RFT, suppliers who formally respond must meet the requirements provided by the company, which outline the security and compliance specifications in greater detail. Their contracts must include:

- Confidentiality clauses
- GDPR compliance
- Defined periodic security audits and right to audit on demand
- Describe the service in detail and its purpose
- Outline each party's responsibility including subcontractor obligations
- Outlined procedures for handling security incidents with defined notification timelines
- Data classification and handling requirements (storage, transfer, disposal)
- Business continuity and disaster recovery provisions

Suppliers must also define service levels that support business continuity objectives and implement appropriate technical and organizational controls. These measures include obtaining the required security certifications, managing access, monitoring security, and safeguarding the network. Compliance with these requirements is assessed either through a questionnaire or another

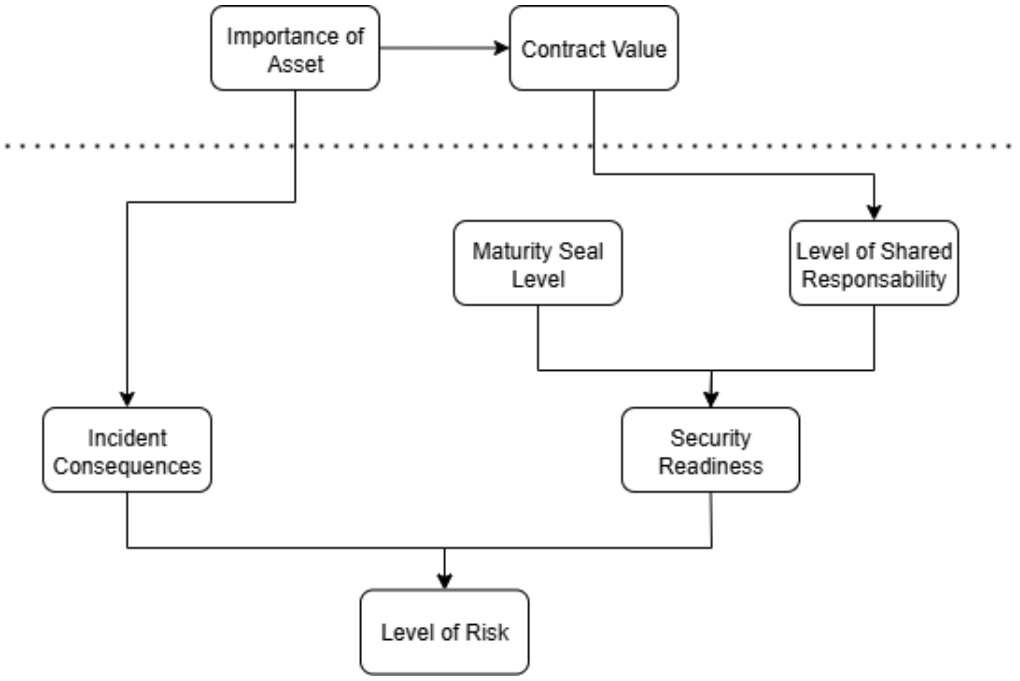

Figure 4.4: Risk Analysis process

method deemed most suitable by the company (An example of a questionnaire is provided in Appendix A.5).

Each asset is assigned a level of importance by the company, and when this significance is aligned with the supplier's compliance with the agreed requirements, it creates a contractual value that clearly outlines the division of responsibilities for the acquisition between the company and the new supplier.

4.5.2 Risk Analysis

The risk under assessment concerns the potential effects that subcontracting a service could have on the organization, evaluated on a per-asset basis. For instance, a supplier's failure to meet compliance requirements might disrupt operations during an incident. The objective of this assessment is to determine whether engaging a third-party provider could benefit or harm the organization, and to what extent. Beyond identifying possible outcomes, the process also supports informed decision-making about whether working with a supplier represents a worthwhile investment.

The risk analysis phase starts only after both parties have established the contractual requirements and assessed the supplier's compliance to risk management maturity through the use of Maturity Seals. A lack of complete information on the identified requirements or insufficient transparency regarding subcontractors, if they impact the asset in question, also presents a risk, indicating potential gaps in trustworthiness and knowledge. Therefore, these factors should be considered when determining the overall risk level. Figure 4.4 outlines the flowchart for the second phase of risk management.

Maturity Seal Level

In developing a comprehensive compliance evaluation model based on the Digital Maturity Seals, it's important to integrate a structured approach that mirrors the intent and structure of the "Regulation of the Digital Maturity Seals" and the "Decree-Law No. 65/2021," while adapting them to the specific objectives of this model.

This model will assess organizations across two pivotal dimensions: Cybersecurity and Privacy and Personal Data Protection. Each dimension is critical in ensuring a holistic transition towards digital maturity, with organizations being rated within a spectrum ranging from Bronze to Gold based on their compliance level.

Certification Process Overview

- **Application Analysis:** An initial review determines the organization's eligibility for certification in one or more designated areas. This step ensures that only organizations with a fundamental commitment to the pillars of digital maturity proceed to a detailed evaluation.
- **Assessment and Audit:** A comprehensive assessment and auditing process in the selected areas to ascertain the level of compliance. This phase is crucial in identifying both the strengths and areas for improvement within the organization's digital practices.
- **Certification Decision and Issuance:** Based on the findings from the assessment and audit, a decision is made on whether the organization meets the necessary criteria for certification. A certificate of compliance is then issued, marking a significant milestone in the organization's journey towards digital maturity.
- **Registration and Seal Application:** The certification is registered on the designated portal, and the Digital Maturity Seal is requested. This formalizes the organization's achievement and allows for public recognition of its compliance.

For each category (Cybersecurity, Privacy and Personal Data Protection) the evaluation criteria is the following:

- **Bronze:** Achieved by organizations that meet the basic requirements set forth in the guidelines. (2 point)
- **Silver:** Granted to organizations that exceed basic requirements, implementing recommended practices and showing above-average results in audits. (3 points)
- **Gold:** Awarded to organizations that demonstrate excellence in compliance, adopt industry-leading practices, and show innovation within the respective areas. (4 points)

Following the evaluation in individual categories, a comprehensive global assessment is conducted, with the following evaluation criteria:

- **Bronze:** A minimum of 4 points, demonstrating digital maturity in at least 2 dimensions.

- **Silver:** A minimum of 7 points, with a silver grade in at least one dimension.
- **Gold:** A minimum of 9 points, with at least a gold grade and a silver grave.

Security Readiness

Security Readiness represents the balance between the supplier's maturity seal level and the distribution of responsibilities within the relationship.. The share of responsabilities parameters used in this approach can be adjusted according to the company's specific needs, ensuring flexibility and relevance to different contexts. This approach is simply a representation and can be tailored to align with the organization's unique risk assessment framework.

Maturity Seal Level	**Share of Responsabilities**				
	Enterprise Extension	Strategic Alliance	Management	Outsourcing	Contract
Gold	Moderate	High	High	High	High
Silver	Low	Moderate	Moderate	High	High
Bronze	Critical	Low	Low	Moderate	Moderate

Table 4.2: Security Readiness assessment

As shown in table 4.2 we will consider 5 types of relationships regarding share of responsibilities:

- **Enterprise Extension:** Full integration with total information sharing for maximum efficiency and stability.
- **Strategic Alliance:** Deep cooperation with shared resources, planning, and long-term efficiency goals.
- **Management:** Leadership-driven collaboration with shared operational and some strategic information.
- **Outsourcing:** Delegation of non-core business functions to external partners for efficiency and cost reduction.
- **Contract:** Basic, short-term collaboration with limited reliance and minimal information sharing.

Security Readiness is categorized into four levels:

- **High:** A resilient and adaptive security posture, where strong compliance meets deep collaboration. Risks are proactively managed, and security is seamlessly integrated into operations, fostering stability and trust.
- **Moderate:** A capable but evolving security stance, where reasonable safeguards exist but may lack full coordination. Some risks are addressed proactively, while others rely on reactive measures, leading to occasional vulnerabilities.

- **Low:** A fragmented security approach, where limited maturity and weak collaboration create inconsistencies. Security efforts are often isolated, risk management is reactive, and gaps in responsibility expose the organization to potential threats.
- **Critical:** An unstable and high-risk environment, where security immaturity and minimal collaboration lead to significant vulnerabilities. Risk is unmanaged, compliance is questionable, and security failures are likely.

Incident Consequences

An asset's incident consequences is determined by its **impact** and **criticality** on an organization's operations, safety, and financial performance. As the consequences and criticality increase, so does the need for effective maintenance, risk mitigation, and resource allocation.

For the incident consequences we will have 4 tiers:

- **Critical:** Immediate failure of multiple operations or systems, no redundancy, requires urgent attention to meet production goals.
- **Significant:** Limits production or shuts down a single system, may have redundancy, issues should be prioritized and scheduled.
- **Moderate:** Affects or shuts down a single system, typically has redundancy or bypass to maintain production.
- **Low:** No immediate impact on capacity, may follow "Run-to-Failure" strategy, addressed through normal workflow processes.

Level of Risk

The contract specifies the risk-related requirements. A third party meets these requirements if its security readiness either aligns with them or mitigates the impact of incidents based on the asset's importance to the company. The level of risk is assessed by considering both the potential consequences of an incident for the company and the supplier's security readiness. For that we have the same 4 levels of risk as the one used in table 4.2.

- **Critical:** A critical risk represents a severe and immediate threat to the organization's operations, security, or reputation. It arises when vulnerabilities are deeply embedded and the organization lacks sufficient safeguards or visibility. These risks demand urgent attention and proactive mitigation, as they can lead to systemic failures, regulatory breaches, or irreversible damage.
- **Significant:** Significant risk indicates a substantial threat that could disrupt operations or compromise sensitive information if not properly managed. While not as urgent as critical risks, these still require prioritized mitigation and continuous monitoring.

- **Moderate:** Moderate risk reflects a manageable level of exposure where existing controls and practices provide a reasonable degree of protection. These risks may cause localized disruptions or inefficiencies but are unlikely to result in major incidents.

- **Low:** Low risk signifies a stable and well-controlled environment where threats are minimal and unlikely to cause significant harm. While they do not require immediate action, they should still be documented and reviewed periodically to ensure continued alignment with evolving business needs and threat landscapes.

Security Readiness	**Incident Consequences**			
	Critical	High	Moderate	Low
Critical	Critical	Critical	High	Moderate
Low	Critical	High	Moderate	Low
Moderate	High	High	Moderate	Low
High	Moderate	Moderate	Low	Low

Table 4.3: Level of Risk assessment

4.5.3 Risk Evaluation

After identifying the risks, the organization must apply its risk acceptance criteria to evaluate whether the overall risk of the asset falls within acceptable limits. The outcome of this evaluation then serves as the basis for deciding whether to proceed with or avoid the acquisition. The activities involved in this evaluation phase are illustrated in Figure 4.5.

Risk levels can be validated through a consensus between the risk owner, the assets risk evaluation, and alignment with the maturity report. It is crucial that risk owners fully understand the risks they are responsible for, based on the assessment findings. Any inconsistencies between the evaluated risk levels and the risk owners perceptions should be analyzed to determine which more accurately represents the actual risk landscape.

The outcome of this phase should be the issuance of a final decision, which will inform decision-making and raise awareness about the organization's risk exposure and the potential impact when engaging a subcontractor. The process of drafting the risk opinion should include:

- A concise summary outlining the identified risk level, the share of responsibilities, and the potential impacts;

- Identification of the responsible area for managing the contractual relationship, ensuring that if the opinion is unfavorable, this area assumes ownership of the associated risks;

The decision should be formally issued and communicated to management and the owner of the relevant contractual relationship. Its conclusions should support the development of an action plan, which may include:

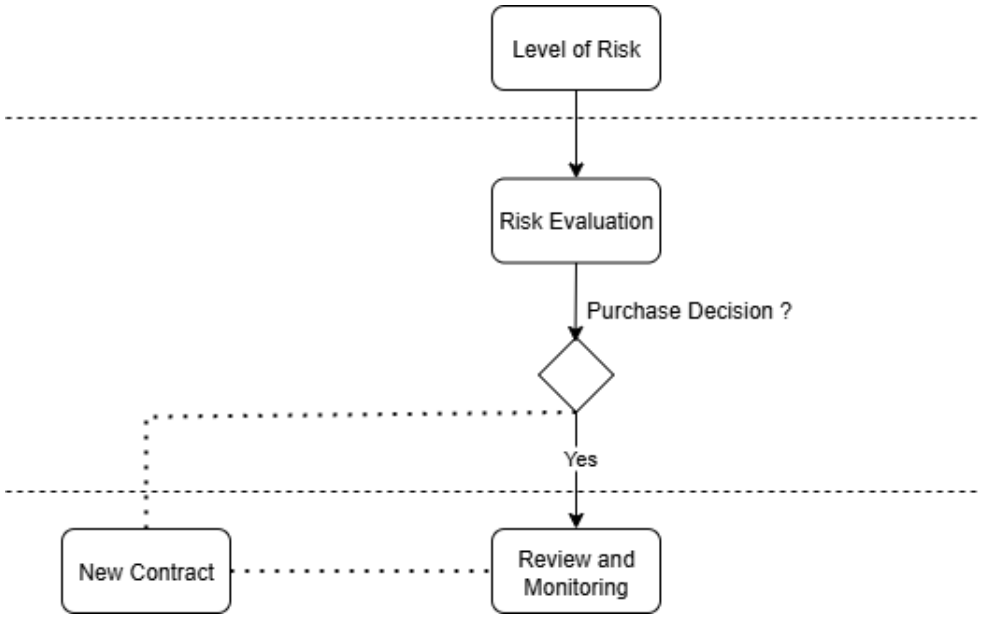

Figure 4.5: Risk Evaluation process

- Proceeding with the contracting, in which case a detailed risk treatment and monitoring plan should be implemented
- Not proceed with the contracting

Once supply chain risk management is completed, we will move into the second part of implementation, focusing on the challenges of transparency and alignment. While the broader framework aims to reduce these risks, this stage introduces a targeted mechanism to address them more directly.

4.5.4 Audit Metrics

Recognizing that suppliers may withhold sensitive information due to competitive, legal, or privacy concerns, audits serve as a critical mechanism to bridge information gaps and enhance transparency in supply chain cybersecurity. By leveraging independent and objective assessments conducted under strict confidentiality agreements, audits provide verifiable assurance of supplier security posture without requiring exhaustive raw data exchange. Auditing programs must be carefully scoped, with contractual enforcement of audit rights, timely incident disclosure, and clear governance to foster alignment and trust among supply chain partners. While audits cannot fully eliminate transparency barriers, when combined with contractual controls (Chapter 3.3) and collaborative communication structures, they substantially mitigate information asymmetry, enabling organizations to manage risk exposures with increased confidence. Ongoing audit program refinement, stakeholder engagement, and monitoring ensure that transparency and alignment improvements are sustainable amid the dynamic nature of supply chains.

Audit Confidentiality and Transparency

Audits, especially **external audits**, serve as a fundamental mechanism to counteract the transparency challenges prevalent in complex supply chains. Given the competitive nature of supplier relationships, sharing sensitive operational or security data is often met with reluctance. External audits, conducted by independent third parties, provide a structured and confidential framework for validating compliance without compromising sensitive information.

This approach promotes trust among all supply chain members by ensuring consistent and unbiased assessments of security practices. Furthermore, contractual clauses requiring the sharing of predetermined audit reports or certifications ensure ongoing transparency. To maintain accountability, policies mandate the reporting of cybersecurity incidents within a strict timeline (e.g., within 48 hours), thus fostering timely and coordinated responses.

Risk-Based Audit Management

Effective audit programmes prioritize resources based on risk exposure and impact potential, aligning with the **risk-based approach** recommended in international standards. This involves focusing audit efforts on the most critical suppliers and components within the supply chain—those whose compromise could have cascading effects on the broader network.

Auditing activities should include regular assessments aligned to risk levels identified in prior risk management phases. This targeted approach improves efficiency by dedicating audit intensity to high-risk areas while reducing unnecessary overhead. Moreover, continuous monitoring enables the detection of emerging risks and supports dynamic adjustments to audit plans, thereby contributing to overall improvement of supply chain cybersecurity maturity.

Stakeholder Roles and Responsibilities

Audit effectiveness depends on clear role definition and coordinated engagement across stakeholders. Different stakeholders require tailored communication and involvement levels:

- **Suppliers** must cooperate fully with auditors, provide evidence of compliance, and rectify findings promptly.
- **Internal audit teams** drive consistency within the organization by conducting regular reviews fostering alignment of practices and response strategies across departments.
- **Audit managers** oversee the planning, execution, and reporting of audit activities, ensuring impartiality and adherence to established audit criteria.
- **Executive leadership and risk owners** rely on audit outcomes for informed decision-making and strategic risk management oversight.

Defining and communicating these roles ensures accountability and reinforces the shared objective of mitigating supply chain risks collaboratively.

Audit Reporting and Metrics

To evaluate audit effectiveness and trace progress in cybersecurity risk management, key performance indicators (KPIs) and metrics must be established. Examples include:

- **Completion rate of audits** across all suppliers and supply chain tiers.
- **Proportion of audits without critical findings**, signaling overall compliance health.
- **Timeliness of incident reporting** relative to contractual expectations.
- **Audit frequency and scope adherence**, ensuring coverage aligns with risk priorities.

Regular reporting of these metrics supports transparency among stakeholders and institutionalizes continuous improvement cycles within the supply chain.

Audit Limitations and Complementary Controls

While audits are powerful tools, their limitations should be acknowledged. Over-reliance can lead to **audit fatigue**, where repetitive or excessive auditing triggers disengagement or complacency among staff. In addition, audits alone cannot prevent **risk compensation** behaviors, where personnel adjust their behavior based on perceived security controls, potentially creating new vulnerabilities.

To address these issues, audits should be supplemented with:

- **Practical risk compensation countermeasures**, such as dual approval mechanisms, task rotations, and scenario-based training.
- **Balanced audit scheduling**, reducing redundancy while maintaining oversight.
- **Integration with other governance, risk management, and compliance (GRC) processes**, embedding audit findings into broader risk treatment plans.
- **Internal controls**, including continuous monitoring, attestation, and real-time security analytics, to complement periodic audit snapshots.

4.6 Improvement Phase

After the risk management process is completed and the company decides to move forward with the acquisition, and once all contractual agreements are finalized, the improvement phase begins. During this stage, attention shifts from transaction execution to operational integration, with a particular focus on evaluating and enhancing supply chain risk maturity.

First, supply chain risk maturity will be assessed against the agreed-upon KPIs, metrics, and goals to establish a clear baseline of performance and resilience. Following the assessment, the

focus will shift to identifying opportunities for improvement, this is particularly critical: supplier networks evolve, new vulnerabilities emerge, and threats change rapidly.

The Improvement Phase therefore establishes a mechanism to regularly assess current practices, benchmark against defined standards, and identify opportunities for enhancement. To operate this cycle, the framework works the concept of Supply Chain Risk Maturity, a structured model that evaluates the organization's progress and defines a roadmap for continuous evolution.

4.6.1 Supply Chain Risk Management Maturity

The Supply Chain Risk Management Maturity Model provides a systematic method for evaluating how well an organization manages risks in its supply chain and for guiding further improvement. Instead of treating risk management as a binary "present or absent" activity, maturity is assessed across levels of sophistication. Each level is defined by specific metrics, which serve as observable indicators of practices, structures, and results.

By applying this model, organizations can:

- Diagnose their current maturity level.
- Identify which requirements are already fulfilled and which are missing.
- Plan targeted actions to move towards higher maturity.
- Achieve gold in all maturity seals criteria

Maturity Levels

The maturity model outlines six progressive stages, moving from informal, ad hoc practices to advanced resilience. Each stage draws on insights mentioned during both the pre-implementation and implementation phases. While a Level 0 can be used to represent the total absence of a supply chain risk management process, it has no interest for the purpose of this framework. At the highest stage, the model connects with the framework's final element, an ongoing cycle of identifying and implementing improvements.

- **Level 1 – Initial (Ad hoc):** Risk practices are inconsistent, undocumented, and highly dependent on individuals. Supplier relationships are not systematically inventoried, and responses to incidents are improvised.
- **Level 2 – Basic Governance:** Basic structures emerge. Roles and resources are assigned, a preliminary supplier list exists, and some contracts include minimal security clauses. Risk monitoring occurs sporadically but lacks consistency.
- **Level 3 – Structured:** Risk management becomes formalized and documented. Supplier mapping, risk criteria, and structured assessments are established. Stakeholder consultation, training, and monitoring plans are systematically integrated.

- **Level 4 – Measured:** The organization adopts quantitative monitoring. SCOR performance attributes are linked to cybersecurity KPIs, dashboards are introduced, and baselines and audits allow for data-driven management.
- **Level 5 – Collaborative:** Risk management transcends organizational boundaries. Suppliers are engaged in joint workshops, intelligence is shared, collaborative incident response is designed, and contracts are updated dynamically.
- **Level 6 – Adaptive/Resilient:** The most advanced stage, where risk management becomes hypothesis-driven and self-renewing. Predictive analytics, simulations, and new KPIs continuously refine practices.

Levels Checklist

The following table presents the detailed set of metrics associated with each level. These metrics serve as the concrete evaluation points to determine maturity

Maturity Phase	Id	Sub-Id	Requirement
Initial (Ad hoc)	1	1	At least one ad hoc supply chain risk or incident report exists.
	1	2	No formal process for supplier cybersecurity risk management is documented.
	1	3	Supplier relationships are tracked informally (no centralized inventory).
	1	4	Incident response to supplier issues is improvised rather than based on defined procedures.
Basic Governance	2	1	A risk manager or responsible role is assigned.
	2	2	Resources are allocated to supplier risk management.
	2	3	A supplier inventory is created and maintained at least partially.
	2	4	Some supplier contracts include basic cybersecurity clauses or service level agreements (SLA).
	2	5	Occasional audits or assessments of suppliers are performed, though inconsistently.
	2	6	Communication of risks to stakeholders (internal/external) occurs but is informal.
Structured	3	1	Organization provides structured training in supply chain cybersecurity risk management.
	3	2	Supplier risk management processes are documented and applied consistently.
	3	3	Risk evaluation criteria (likelihood, impact, thresholds) are defined.
	3	4	Risk management objectives are aligned with organizational objectives.
	3	5	Supplier mapping (e.g., SCOR model or equivalent) is used to identify risk points.
	3	6	All significant suppliers are subject to risk assessment.

Maturity Phase	Id	Sub-Id	Requirement
	3	7	Identified risks are documented in a centralized risk register.
	3	8	Each risk has an assigned owner.
	3	9	Procedures exist for identifying positive risks (opportunities).
	3	10	Risk analysis is carried out systematically (qualitative or semi-quantitative scoring).
	3	11	Risk evaluation compares assessed risks against defined criteria.
	3	12	Risk treatment decisions are prioritized and documented.
	3	13	Stakeholder consultation and communication follow a structured plan.
	3	14	Regular monitoring and review of supplier risks is scheduled and documented.
Measured	4	1	Supply chain risk KPIs are defined (e.g., supplier compliance rate, incident frequency).
	4	2	SCOR performance attributes (reliability, responsiveness, agility, cost, asset efficiency) are linked to risk indicators.
	4	3	Dashboards or reporting systems track supplier cybersecurity risk.
	4	4	Baselines for supplier performance and incident frequency are established.
	4	5	Key Risk Indicators are tracked regularly.
	4	6	Statistical methods are used to evaluate supplier risk trends.
	4	7	Supplier SLA compliance is quantitatively monitored.
	4	8	Supplier performance in audits is scored and trended over time.
	4	9	Independent reviews or third-party audits are conducted systematically.
	4	10	Performance deviations trigger corrective management actions.
Collaborative	5	1	Joint supplier–organization risk workshops are conducted.
	5	2	Cybersecurity intelligence is shared between the organization and its critical suppliers.
	5	3	Collaborative incident response plans are developed with key suppliers.
	5	4	Industry standards or best practices are co-developed with suppliers/partners.
	5	5	Regular benchmarking of supply chain risk management against peers or industry.
	5	6	Continuous improvement actions are applied across supplier relationships.
	5	7	Supplier development programs (e.g., training suppliers) are in place.
	5	8	Contracts are regularly reviewed and updated to reflect evolving risk requirements.
	5	9	Cross-functional teams (procurement, IT, security, compliance) collaborate in supplier risk management.
	5	10	Supplier maturity levels are monitored and actively raised through collaboration.

Maturity Phase	Id	Sub-Id	Requirement
Adaptive/Resilient	6	1	Predictive analytics are used to anticipate supply chain cyber risks.
	6	2	Regular simulations/stress-tests are conducted to evaluate supply chain resilience.
	6	3	Hypothesis-driven improvements are piloted (e.g., testing new scoring or monitoring methods).
	6	4	New KPIs and metrics are regularly generated and refined.
	6	5	Automated or semi-automated adaptive controls are implemented in supplier oversight.
	6	6	Active participation in cross-industry collaborations and information-sharing ecosystems.

Table 4.4: Evaluation Metrics by level

To be assigned maturity Level N, an organization must atisfy all requirements of Levels 1…N–1. Early adoption of higher-level practices may be recorded, but the assigned maturity cannot exceed the highest level whose prerequisites are met. The maturity levels are structured in a progressive manner, which means that while it is possible to meet some of the criteria of a higher level, it is not possible to complete all of them without first fulfilling the requirements of the levels below.

Each organization is responsible for defining, within its supplier-risk policy, the specific acceptance criteria for each maturity level. The set of metrics provided in this model is intended as a best-fit general framework; however, organizations are expected to tailor these metrics to their own operational and risk management context. As such, certain metrics may be added, removed, or adapted to ensure relevance and applicability, while maintaining consistency and transparency in how maturity is assessed.

Use Cases

To illustrate how the proposed maturity model can be operationalized, Table 4.5 and Table 4.6 use cases are provided. These examples demonstrate how individual metrics from the model can be transformed into structured evaluation items.

ID	3.7
Title	Centralized Risk Register
Purpose	The purpose is to determine whether identified supplier-related risks are systematically documented and maintained in a centralized risk register accessible to relevant stakeholders.
Notes	A risk register should contain information such as risk description, owner, likelihood, impact, treatment, and current status. The centralization of this information ensures traceability, accountability, and consistency in supplier risk management processes across the organization.
Answers	No: Risks are documented in an ad hoc or fragmented manner.
	Yes: All identified risks are documented in a centralized risk register.
Source	Adapted from ISO 31000:2018 – Risk Management Guidelines [31]

Table 4.5: Use Case 1 – Centralized risk register (Level 3, Structured)

ID	5.2
Title	Cybersecurity Intelligence Sharing
Purpose	The purpose is to assess whether the organization and its critical suppliers actively share cybersecurity threat intelligence and incident information to enhance collective resilience.
Notes	Information-sharing can occur through joint threat reports, alerts, workshops, or participation in sectoral information-sharing and analysis centers (ISACs). The goal is to improve situational awareness and strengthen the overall supply chain security posture.
Answers	No: Cybersecurity intelligence is not systematically shared with suppliers.
	Yes: Cybersecurity intelligence is actively shared with critical suppliers.
Source	Adapted from NIST SP 800-161r1 – Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations [48]

Table 4.6: Use Case 2 – Cybersecurity intelligence sharing (Level 5, Collaborative)

4.6.2 Continuity Plan

The objective of the continuation plan is to enhance the overall maturity of supply chain cybersecurity risk management in a sustainable and progressive manner. This plan functions as a strategic roadmap that guides ongoing efforts to elevate the risk posture of the entire supply chain, ensuring that maturity advancements are enduring and responsive to evolving threats and business contexts.

To achieve this objective, organizations must implement ongoing activities that support the sustained advancement of maturity, including:

- **Regular Assessment and Benchmarking:** Continuously evaluate supply chain risk management practices against established KPIs, performance metrics, and maturity model criteria. This evaluation helps identify gaps, strengths, and evolving risks, providing a clear picture of current maturity levels.
- **Feedback Loops and Learning:** Create mechanisms for gathering insights and lessons learned from audits, incident responses, and risk treatment outcomes. Integrating this knowledge into policy updates, training programs, and process refinement accelerates maturity improvement.
- **Adaptation to Changing Threat Landscapes:** The dynamic nature of cyber threats and supply chain structures requires organizations to remain agile. Continuous monitoring of emerging vulnerabilities, supplier changes, and technological advancements ensures that risk management practices evolve accordingly.
- **Stakeholder Engagement and Collaboration:** Foster strong collaboration within and across organizational boundaries, including suppliers and partners. Promoting transparency and aligning on cybersecurity goals enhances trust and shared responsibility—key drivers of maturity.
- **Governance and Accountability:** Maintain robust governance structures that assign clear ownership and responsibility for continuous improvement initiatives. Executive sponsorship and cross-functional teams ensure strategic alignment and resource commitment necessary for sustained progress.

Chapter 5

Analysis and Evaluation

This chapter demonstrates the application of the framework introduced earlier through a fictional use case. As the scenario is purely illustrative, the examples of tools, algorithms, event logs, and models are limited in scope and not intended to represent complete or valid inputs. In addition, not every step of the framework is described in full detail, since such depth would only be possible in a real-world implementation within an organization.

The framework is not intended to be prescriptive; rather, it is designed to be adaptable to the unique characteristics and requirements of each organization. Depending on the context, companies may choose to add new activities, refine existing ones, or remove certain steps altogether, ensuring that the model remains aligned with their strategic objectives, available resources, and operational constraints.

5.1 Use Case

Company A, a multinational IT provider, faced growing limitations in its internal Security Operations Center, particularly in its ability to detect incidents quickly, manage continuous monitoring at scale, and comply with strict regulatory reporting obligations. At the outset, processes were fragmented, with incident logs scattered across business units, partial manual triage still in use, and supplier relationships not recorded in any centralized inventory. In practical terms, the organization was operating at what the maturity framework would classify as Level 1 – an ad hoc posture that relied heavily on individual expertise rather than on formal governance.

In order to reinforce its capacity, Company A decided to outsource SOC services to an external provider, referred to as Supplier B, a managed security services provider specializing in 24/7 monitoring and incident response. Supplier B's own operations, however, depended on several upstream partners, including cloud providers for data processing and log storage, threat intelligence feed vendors, and subcontracted first-line analysts. This multi-tier landscape meant that the risk profile extended well beyond the direct relationship: Company A's cybersecurity resilience would be influenced not only by the chosen supplier's practices but also by those of its partners further up the chain.

Before proceeding to negotiations, requirements were gathered and translated into a formal

request for tender. These included compliance with GDPR in cross-border data management, the obligation to provide immediate traceability of security incidents, incident reporting within a maximum of four hours, and visibility into Tier-2 dependencies. Candidate providers were evaluated using the proposed maturity seals system, where Supplier B achieved a silver rating: compliant with most best practices, yet with limited transparency across its own subcontractors.

The identification of risks was therefore prioritized. Company A recognized that the most significant operational risks were associated with the possibility of cloud outages disrupting log access, compliance risks arising from improper handling of personal data, and dependency risks stemming from the concentration of monitoring responsibilities in a single MSSP. A financial concern was also noted, since unforeseen costs could surface during integration. Each of these risks was recorded in a newly created risk register, marking one of the first signs that the organization was beginning to move away from informal handling toward more structured documentation.

The subsequent analysis relied on qualitative evaluation. For example, a potential cloud outage was judged to be moderately likely but of high impact, while GDPR violations were assessed as unlikely but catastrophic in consequence. The financial risk of cost overruns was considered possible, though with only moderate impact. Conformance checking revealed that Supplier B, while contractually committing to a four-hour detection time, had in some pilot cases actually delivered alerts in six to seven hours. This deviation made explicit the need for stricter governance provisions in the contract, including penalties for SLA breaches.

At this stage the organization faced two trade-off decisions. On the dependency risk side, managers weighed the option of trusting a single MSSP without redundancy, which would keep costs down but leave the organization exposed to systemic failures, against investing in redundant log storage across multiple European cloud regions. While the second option raised contract costs by about twelve percent, it reduced dependency risk from high to moderate and was therefore chosen. On the compliance side, accepting Supplier B’s internal policies without verification would have left GDPR risk critical, so the company instead opted to include explicit audit rights and a mandatory incident reporting time of forty-eight hours, reducing the risk classification to significant.

The contract was then finalized with these risk treatments integrated: SLA penalties for delays in detection, detailed data protection clauses, audit rights extending into critical Tier-2 subcontractors, and an exit strategy guaranteeing transfer to an alternative provider in case of severe or repeated failures. Monitoring arrangements were formalized around monthly performance reporting, quarterly joint incident simulations, and biannual external audits, thus embedding continuous oversight into the lifecycle of the agreement.

After six months of operation, measurable results were recorded. The mean time to detect incidents had decreased from eight hours to around two and a half, SLA compliance had risen to ninety-eight percent, Tier-2 visibility had improved with a forty percent reduction in opaque dependencies, and the risk register now documented one hundred percent of critical suppliers. These results confirmed that the outsourcing initiative effectively served as a catalyst for moving

the organization's maturity level to Level 3 – structured. While some practices, such as dashboards for quantitative tracking and intelligence sharing, remained in development, the chain had clearly progressed beyond its previous reactive posture.

The case therefore demonstrated that outsourcing did not merely transfer risk to an external provider but, if structured within a formal maturity framework, could become an instrument of governance improvement. Company A's relationship with Supplier B exemplifies how the acquisition of a critical cybersecurity service, when combined with contractual rigor and a systematic risk management methodology, can advance an entire organization from fragmented, ad hoc processes toward structured and evolving maturity.

5.2 Evaluation

To validate the proposed maturity framework for supply chain cybersecurity risk management, we conducted a structured interview with an expert in the field. The participant, referred to as X, currently serves as a coordinator in Governance, Risk, and Compliance (GRC) at a Portuguese major retail company. With more than 10 years of professional experience, X has built expertise in incident and vulnerability management, identity management, ISO-based audits, and privacy by design/default. Earlier in their career, X worked in the energy sector, focusing on information security operations, and later specialized in security assessments and privacy risk management. For the past six to seven years, X has led a GRC team, developing a "security by design" framework grounded in ISO 27001/27002 standards and adapted to GDPR requirements. Their work spans IT risk assessment for applications and third parties, compliance with evolving regulations such as NIS2 [14], and oversight of audits. Key responsibilities include evaluating risks tied to critical assets, assessing third-party contractual obligations and shared responsibilities, and monitoring incident-related risks. Through this role, X ensures the alignment of regulatory, technological, and organizational requirements to strengthen overall cybersecurity resilience.

When asked about maturity practices, X explained that although the company does not follow a formally certified maturity model (such as CMMI or the National Cybersecurity Center's maturity framework), internal controls are structured around ISO standards and GDPR requirements. A set of controls is applied consistently, adapted to the specific scope (applications or third parties), and complemented by contractual clauses and continuous monitoring. Maturity, therefore, is assessed in a practical sense, though not via a standardized framework.

The expert confirmed that transparency, accountability and alignment remain critical challenges in supply chain risk management. X emphasized the importance of clearly assigning accountability, referencing the "A" in a RACI matrix. Internally, X noted that contracting processes must begin with the Legal department, which plays a central role in guiding risk assessments and clarifying responsibilities. For suppliers, X's team does not directly manage communication but rather provides risk-oriented evaluations, leaving contractual engagement to business or IT owners. However, X's team ensures that risk assessments are incorporated into contracting decisions, particularly for critical suppliers and services that fall under new regulatory obligations

(e.g., NIS2).

Regarding the pre-implementation phase of the proposed framework, X highlighted the value of asset awareness and prioritization, agreeing that such an approach strengthens decision-making and clarifies organizational needs. X supported the introduction of a structured model like SCOR to formalize subcontracting decisions, noting that aligning expected inputs and outputs would improve efficiency.

When discussing the implementation phase, X acknowledged the potential usefulness of maturity "seals" for supplier evaluation but remarked that such seals are not yet widely available in practice. Instead, organizations tend to rely on certifications, contractual requirements, and internal checklists. X observed that in many real-world cases, procurement may be limited to a single supplier option, which reduces the applicability of idealized selection processes. Still, X agreed that defining responsibilities and assessing supplier dependency are crucial.

On the subject of transparency and strategic alignment at the contracting stage, X underlined the importance of including clear technical and organizational measures (TOMs) and audit clauses in contracts. X agreed that audit fatigue is a risk but suggested a criticality-based approach: partners with higher risk profiles or incident histories should be prioritized for audits or periodic assessments. The experts organization uses annual questionnaires for critical suppliers as a lighter alternative to formal audits. While acknowledging limitations in budget and resources, X confirmed that contract clauses granting audit rights are an effective baseline safeguard.

In response to the improvement phase of the framework, X stressed that reassessment of maturity should follow actual execution of contracts and improvement actions. The expert saw the model as aligned with the ISO concept of the Statement of Applicability (SoA), where controls and maturity assessments are iteratively refined. X emphasized that improvements could involve not only external contracting but also internal initiatives such as training or team restructuring. The expert agreed with the notion of continuous evaluation at periodic intervals (e.g., every three, six, or nine months) and confirmed that this reflects real practices within his organization.

X also offered reflections on external collaboration. While internal controls dominate current practice, the expert noted that initiatives are emerging to encourage inter-organizational cooperation, such as group-level knowledge sharing and vulnerability reporting encouraged by national cybersecurity authorities. X considered the idea of centralized maturity seals or pre-assessed "trusted partners" valuable, as it could increase trust in third-party relationships and reduce redundancy in evaluations.

5.3 Revised Model

During the expert interview, it was highlighted the importance of a stage between the contract celebration and the subsequent maturity review. The overall framework remained unchanged however, the revised model, demonstrated in Figure 5.1 introduced an additional step (Observation of Contract) within the improvement phase.

In this step, the focus shifts from the metrics initially expected as a consequence of the contract

to the metrics that are actually observed once the contract is in effect. The duration of this observation period may extend as long as the organization deems appropriate, after which the Evaluation Against Metrics should be conducted. The inclusion of this stage illustrates the premise that the practical application of the contractual relationship is necessary to reveal concrete developments, as opposed to merely theoretical or projected outcomes.

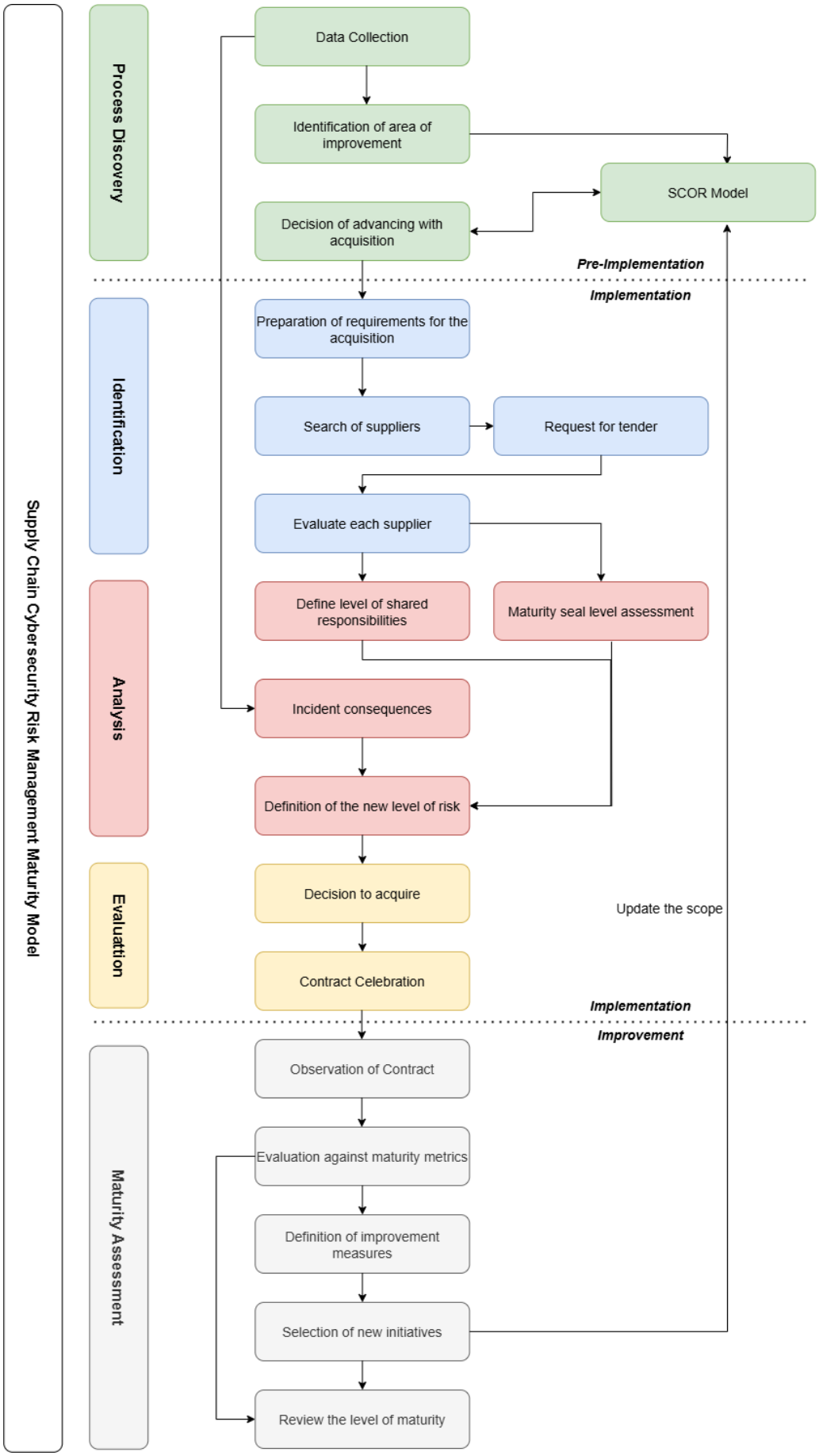

Figure 5.1: Revised Model

Chapter 6

Conclusion and Future Work

This chapter presents the study's conclusions, acknowledges its limitations, and offers insights to guide future work.

6.1 Conclusions

This research set out to address a critical gap identified in the literature review: the lack of an integrated, practical framework for assessing and advancing Supply Chain Cybersecurity Risk Management Maturity (SCCRMM) across multi-tier supply networks. The study aims to close the divide between the growing complexity of supply chains and the need for a maturity-driven framework that delivers tangible organizational value.

To this end, it introduces a conceptual framework built on three core pillars: SCOR-based process discovery, a standards-aligned risk management workflow, and auditing. Combined within a maturity-focused approach, these elements provide a comprehensive method for managing cybersecurity risks in supply chains. The framework promotes transparency and alignment across chain partners, incorporates maturity "seals" for supplier assessment in cybersecurity and privacy, and grounds improvement efforts in measurable KPIs and audit metrics. Collectively, these components offer a structured pathway for progressively and sustainably enhancing risk resilience across the supply chain. To illustrate the approach, a fictional use case is presented, and to validate the framework, an expert interview was conducted.

This thesis makes several important contributions. It integrates risk maturity models into supply chain cybersecurity risk management, explores the cybersecurity challenges that emerge at this intersection, such as audit fatigue, and building on this foundation, proposes a holistic SCCRMM framework. The framework offers a structured, step-by-step methodology adaptable to diverse organizational contexts and resource levels. By doing so, it equips stakeholders to strengthen processes with modern techniques while maintaining clarity of purpose, intent, and traceability.

6.2 Limitations and Future Work

The work assumes that an organization or the stakeholders on a supply chain are capable of assessing its level of maturity in supply chain cybersecurity risk management. It further assumes the use of maturity seals to evaluate compliance, while allowing for other suitable methods if deemed appropriate.

One limitation of this study is the scarcity of comparable frameworks in the same domain. While this points to the need for the proposed approach, it prevents meaningful benchmarking against prior work, an appraisal that would have strengthened the validation of our assumptions and methodological choices. The proposed framework was not tested or applied in a real-world scenario, which would have allowed for clearer conclusions about the model's evaluation and review.

A further limitation is the study's exclusively qualitative scope; a robust quantitative evaluation would require a real-world implementation to generate measurable outcomes and allow statistical validation. In addition, the framework does not explicitly address emerging challenges posed by artificial intelligence, both the use of predictive models for risk management and the growing, enterprise-wide adoption of AI systems.

Bibliography

[1] Association for Supply Chain Management (ASCM). Educational videos — supply chain learning center.

[2] Maria Bada and Jason RC Nurse. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes). *Information & Computer Security*, 27(3):393–410, 2019.

[3] Jörg Becker, Ralf Knackstedt, and Jens Poeppelbuss. Developing maturity models for it management. *Business Information Systems Engineering*, 1:213–222, 06 2009.

[4] Peter Bolstorff and Robert G Rosenbaum. *Supply chain excellence: a handbook for dramatic improvement using the SCOR model*. AMACOM/American Management Association, 2012.

[5] Niels Bugert and Rainer Lasch. Supply chain disruption models: A critical review. *Logist. Res.*, 11:5, 2018.

[6] The CMMI Product Team. Cmmi for development, version 1.3. Technical Report CMU/SEI-2010-TR-033, Nov 2010. Accessed: 2024-Dec-2.

[7] Jason Deane, Wade Baker, and Loren Rees. Cybersecurity in supply chains: quantifying risk. *Journal of Computer Information Systems*, 63(3):507–521, 2023.

[8] Gul Esin Delipinar and Batuhan Kocaoglu. Using scor model to gain competitive advantage: A literature review. *Procedia - Social and Behavioral Sciences*, 229:398–406, 2016. 5th International Conference on Leadership, Technology, Innovation and Business Management 2015, ICLTIBM 2015, 10-12 December 2015, Istanbul, Turkey.

[9] Scott Dellana, William J Rowe, and Ying Liao. A scale for measuring organizational risk management maturity in the supply chain. *Benchmarking: An International Journal*, 29(3):905–930, 2022.

[10] Carina Dios Falk. Cyber supply chain security and the swedish security protected procurement with security protective agreement, 2023.

[11] Scott DuHadway, Steven Carnovale, and Vijay R. Kannan. Organizational communication and individual behavior: Implications for supply chain risk management. *Journal of Supply Chain Management*, 54(4):3–19, 2018.

[12] Shannon Leigh Eggers. Towards a new supply chain cybersecurity risk analysis technique. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States), 2021.

[13] Dominique Estampe, Samir Lamouri, Jean-Luc Paris, and Sakina Brahim-Djelloul. A framework for analysing supply chain performance evaluation models. *International journal of production economics*, 142(2):247–258, 2013.

[14] European Parliament and Council of the European Union. Directive (eu) 2022/2555 of the european parliament and of the council 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). Official Journal of the European Union, 2022. OJ L 333, 27.12.2022.

[15] Eurostat. Statistics on small and medium-sized enterprises. *Eurostat*, 2015.

[16] Robert L Freas, Heather F Adair, and Eman Hammad. An engineering process framework for cybersecurity incident response assessment. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8. IEEE, 2022.

[17] Derek Friday and Steven Melnyk. New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, 60, 10 2021.

[18] Toby A Gardner, Magnus Benzie, Jan Börner, Elena Dawkins, Stephen Fick, Rachael Garrett, Javier Godar, A Grimard, Sarah Lake, Rasmus K Larsen, et al. Transparency and sustainability in global commodity supply chains. *World Development*, 121:163–177, 2019.

[19] Abhijeet Ghadge, Maximilian Weiß, Nigel D Caldwell, and Richard Wilding. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, 25(2):223–240, 2020.

[20] Jury Gualandris, Annachiara Longoni, Davide Luzzini, and Mark Pagell. The association between supply chain structure and transparency: A large-scale empirical study. *Journal of Operations Management*, 67, 05 2021.

[21] João Guerra, Fernando Souza, Silvio Pires, and Anderson Sá. A maturity model for supply chain risk management. *Supply Chain Management: An International Journal*, 29, 07 2023.

[22] Nikhil Gupta, Akash Tiwari, Satish TS Bukkapatnam, and Ramesh Karri. Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks. *IEEE Access*, 8:47322–47333, 2020.

[23] Amulya Gurtu and Jestin Johny. Supply chain risk management: Literature review. *Risks*, 9(1):16, 2021.

[24] Margareta Heidt, Jin P. Gerlach, and Peter Buxmann. Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, 21(6):1285–1305, December 2019.

[25] Adam Henschke and Shannon Brandt Ford. Cybersecurity, trustworthiness and resilient systems: guiding values for policy. *Journal of Cyber Policy*, 2(1):82–95, 2017.

[26] Samuel H. Huan, Sunil K. Sheoran, and Ge Wang. A review and analysis of supply chain operations reference (scor) model. *Supply Chain Management: An International Journal*, 9(1):23–29, 02 2004.

[27] ASCM Insights. Circular supply chains will shift scor supply chain processes. *ASCM Insights*, 2024.

[28] ISO/IEC. 15048-1 - information security, cybersecurity and privacy protection — evaluation criteria for it security — part 1 - requirements. 2018.

[29] ISO/IEC. 19011 - guidelines for auditing management systems. 2018.

[30] ISO/IEC. 27000 - information technology — security techniques — information security management systems — overview and vocabulary. 2018.

[31] ISO/IEC. 31000 - risk management — guidelines. 2018.

[32] ISO/IEC. 27036-1 - cibersecurity - supplier relationships - part 1: Overiew and concepts. 2021.

[33] ISO/IEC. 27001 - information security, cybersecurity and privacy protection — information security management systems — requirements. 2022.

[34] ISO/IEC. 27002 - information security, cybersecurity and privacy protection — information security controls. 2022.

[35] ISO/IEC. 27005 - information security, cybersecurity and privacy protection – guidance on managing information security risks. 2022.

[36] ISO/IEC. 27036-2 - cybersecurity — supplier relationships — part 2: Requirements. 2022.

[37] ISO/IEC. 27036-3 - cybersecurity — supplier relationships — part 3: Guidelines for hardware, software, and services supply chain security. 2023.

[38] Yoon Hee Kim and Darren Henderson. Financial benefits and risks of dependency in triadic supply chain relationships. *Journal of Operations Management*, 36:115–129, 2015.

[39] Michael Kohlegger, Michael, Stefan Thalmann, Stefan, Ronald Maier, and Ronald. Understanding maturity models. results of a structured content analysis. 01 2009.

[40] Ravdeep Kour, Ramin Karim, and Adithya Thaduri. Cybersecurity for railways–a maturity model. *Proceedings of the institution of mechanical engineers, Part F: Journal of Rail and Rapid Transit*, 234(10):1129–1148, 2020.

[41] Elisa Kusrini, Tifa Ayu Praditya, and Bayu Wahyudi. Risk maturity model: A systematic literature review'. In *Proceedings of the International Conference on Industrial Engineering and Operations Management (IEOM 2023)*, pages 368–377, 2023.

[42] Eftychia Lakka, George Hatzivasilis, Stylianos Karagiannis, Andreas Alexopoulos, Manos Athanatos, Sotiris Ioannidis, Manolis Chatzimpyrros, Grigoris Kalogiannis, and George Spanoudakis. Incident handling for healthcare organizations and supply-chains. In *2022 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–7. IEEE, 2022.

[43] Yutong Liu, Jian Du, Taewon Kang, and Mingu Kang. Establishing supply chain transparency and its impact on supply chain risk management and resilience. *Operations Management Research*, pages 1–15, 2024.

[44] Marianthi Theocharidou Maria Papaphilippou, Konstantinos Moulinos. Good pratices for supply chain cibersecurity. *ENISA*, 2023.

[45] C. Peters J. Spruill Melnyk, S. A. and K. W. Sullivan. Implementing cybsersecurity in dod supply chains. *White Paper*, 2018.

[46] Claudio Minerbo, Barbara B Flynn, Susana Carla Farias Pereira, and Ryan Outlaw. Supply chain trust: a two-way street? 2018.

[47] NATF. Supply chain security assessment model. *NATF*, 2023.

[48] National Institute of Standards and Technology. Cybersecurity supply chain risk management practices for systems and organizations. NIST Special Publication 800-161r1, National Institute of Standards and Technology, May 2022.

[49] New Zealand Government NCSC National Cyber Security Centre. Supply chain cyber security: In safe hands. 2022.

[50] Jürgen Neises, George Moldovan, Thomas Walloschke, and Bianca Popovici. Trustworthiness in supply chains: A modular extensible approach applied to industrial iot. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE, 2020.

[51] Cherilyn Pascoe. Initial summary analysis of responses to the request for information evaluating and improving cybersecurity resources: The cybersecurity framework and cybersecurity supply chain risk management. 2022.

[52] Mehrdokht Pournader, Andrew Kach, and Srinivas Talluri. A review of the existing and emerging topics in the supply chain risk management literature. *Decision sciences*, 51(4):867–919, 2020.

[53] Diogo Proença, João Estevens, Ricardo Vieira, and José Borbinha. Risk management: A maturity model based on iso 31000. In *2017 IEEE 19th Conference on Business Informatics (CBI)*, 2017.

[54] Karen Renaud, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security*, 78:198–211, 2018.

[55] George Sharkov. Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal*, 19(4):5–24, 2020.

[56] Gordon Stewart. Supply-chain operations reference model (scor): the first cross-industry framework for integrated supply-chain management. *Logistics Information Management*, 10(2):62–67, 04 1997.

[57] Ha Ta, Terry L Esper, Kenneth Ford, and Sebastian Garcia-Dastuge. Trustworthiness change and relationship continuity after contract breach in financial supply chains. *Journal of supply chain management*, 54(4):42–61, 2018.

[58] Constantine Toregas, Joost Santos, Molly Jahn, William L Oemichen, Gregory F Treverton, Scott L David, Matthew A Rose, COL Max Brosig, William K Hutchison, Braeden Rimestad, et al. Cybersecurity and its cascading effect on societal systems.

[59] Johan Turell, Fei Su, and Vincent Boulanin. Cyber-incident management: identifying and dealing with the risk of escalation. *SIPRI: Stockholm International Peace Research Institute*, 2020.

[60] Juneho Um and Neungho Han. Understanding the relationships between global supply chain risk and supply chain resilience: the role of mitigating strategies. *Supply Chain Management: An International Journal*, 26(2):240–255, 2021.

[61] Verónica H. Villena and Dennis A. Gioia. On the riskiness of lower-tier suppliers: Managing sustainability in supply networks. *Journal of Operations Management*, 64:65–87, 2018.

[62] Charles Weber, Mark Paulk, Cynthia Wise, and James Withey. Key practices of the capability maturity model. Technical report, Carnegie Mellon University, 08 1993.

[63] Pascal Wichmann, Alexandra Brintrup, Simon Baker, Philip Woodall, and Duncan Mcfarlane. Extracting supply chain maps from news articles using deep neural networks. *International Journal of Production Research*, 58:1–17, 02 2020.

[64] Pei Xu, Joonghee Lee, James R Barth, and Robert Glenn Richey. Blockchain as supply chain technology: considering transparency and security. *International Journal of Physical Distribution & Logistics Management*, 51(3):305–324, 2021.

[65] Cyndi Man Zhang and Henrich R. Greve. Delayed adoption of rules: A relational theory of firm exposure and state cooptation. *Journal of Management*, 44(8):3336–3363, 2018.

Appendix A

Concepts for the Framework

A.1 Evaluation concepts and relationships

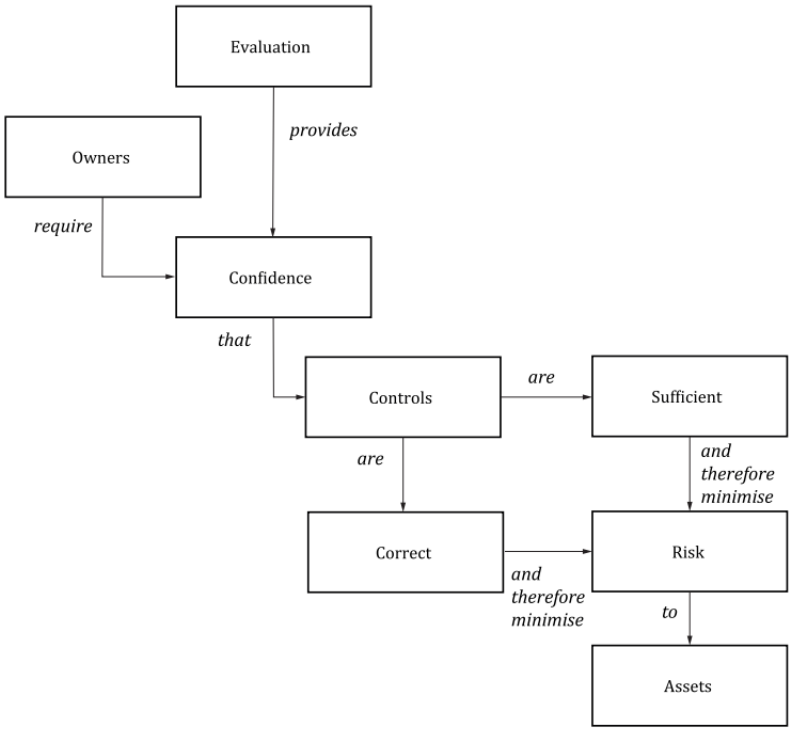

Figure A.1: Evaluation concepts and relationships according to ISO/IEC15048-1:2022[28]

A.2 Controls Layout

According to ISO/IEC27002:2022[34] the layout for each control contains the following:

- **Control title:** Short name of the control;
- **Attribute table:** A table shows the value(s) of each attribute for the given control
- **Control:** What the control is

- **Purpose:** Why the control should be implemented
- **Guidance:** How the control should be implemented
- **Other Information:** Explanatory text or references to other related documents

A.3 Risk Assessment Qualitative Approach

A.3.1 Consequences Scale

The consequence criteria outlined in ISO/IEC 27005:2022[35] specify how an organization may assess the importance of potential information security events. An example provided in Annex A.1.1.2.1 of the standard afore mentioned illustrates a qualitative five-level scale:

Consequences	Description
5 - Catastrophic	Sector or regulatory beyond the organization
4 - Critical	Disastrous consequences for the organization
3 - Serious	Substantial consequences for the organization
2 - Significant	Significant but limited consequences for the organization
1 - Minor	Negligible consequences for the organization

Table A.1: Example of consequences scale according to ISO27005:2022[35]

A.3.2 Likelihood Scale

The likelihood criteria described in ISO/IEC 27005:2022[35] define how an organization can evaluate the probability of a specific risk scenario occurring. Annex A.1.1.2.2 of the standard provides an example using a qualitative five-level scale:

Likelihood	Description
5 - Almost Certain	The likelihood of the risk scenario is very high
4 - Very Likely	The likelihood of the risk scenario is high
3 - Likely	The likelihood of the risk scenario is significant
2 - Rather Unlikely	The likelihood of the risk scenario is low
1 - Unlikely	The likelihood of the risk scenario is very low

Table A.2: Example of likelihood scale according to ISO27005:2022[35]

A.4 ICT Supply chain Risk

According to ISO/IEC 27036-1[32] specific information security risks to an acquirer's and a supplier's information and systems often branch from insufficient control awareness, unclear ownership, and lack of accountability. These risks can arise in the supply of both products and services.Table A.3 illustrates examples of information security risks linked to product acquisition. On the other hand, risks associated with services typically emerge from a supplier's access to the

acquirer's information or systems. Table A.4 highlights examples of such risks related to supplier access.

A.4.1 Risks for acquiring products

No.	Type	Description
1	Information security feature	In the case where supplied products have a vulnerability, the acquirer's derived products, services or processes will be vulnerable.
2	Quality	Poor quality of supplied products can cause information security weakness of the acquirer's derived products, services and processes.
3	Intellectual property rights	Unidentified intellectual property rights can cause later dispute in relation with the acquirer's derived products or services.
4	Authenticity	In the case where fake or fraudulent products were supplied, the acquirer's expectation for an information security feature and the quality and identification of intellectual property rights are threatened with a likelihood of an information security weakness introduced and a loss in the business relationship confidence.
5	Assurance	Without assurance of appropriate information security features, product quality, and identification of intellectual property rights and authenticity, the acquirer lacks confidence in reliance upon the supplier's products.

Table A.3: Example of information security risks for acquiring products based on ISO/IEC27036[32]

A.4.2 Risks for acquiring services

No.	Type	Description
1	Physical Acess Onsite	Supplier has physical acess to the information processing facilities of the acquirer but does not have logical acess
2	Acess to information and information systems onsite	Supplier personnel are onsite and have logical access to information and information systems of the acquirer, through the use of acquirer's equipment
3	Remote acess to in-house information and information systems	Supplier has remote access to information and information systems of the acquirer
4	Processing of information offsite	Information under the responsibility of the acquirer is processed by the supplier offsite, using applications and systems under the control and the management of the supplier
5	Applications offsite	Applications operated by the acquirer are running PaaS or IaaS
6	Equipment offsite	Equipment dedicated to the acquirer and owned by the acquirer are hosted offsite, on the supplier site
7	Storage of information offsite	Acquirer outsources the storage of information to a supplier for offsite retention or archive
8	Source code escrow	Services involving supplier artefacts used by the acquirer are held in escrow by a trusted third party and are made available to the acquirer under defined

Table A.4: Example information security risks for acquiring services based on ISO/IEC27036[32]

A.5 Example of Compliance Questionnaire

Code	Question
SCM-01	Describe how you perform security assessments of third-party companies with which you share data (i.e., hosting providers, cloud services, PaaS, IaaS, SaaS, AI services, etc.). Provide a summary of your practices and/or controls that assure the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.
SCM-04	Do you have an established program that ensures suppliers comply with your organization's security policies and procedures?
SCM-06	Do you have a process by which you verify and validate security updates received from suppliers?
SCM-07	Have you established and do you maintain a program to manage supply chain risks to critical components or services?
SCM-09	Do you have a process by which you will notify customers of security issues or vulnerabilities that may affect supplied components or services?
RISK-05	Do you have a process through which you investigate supply chain incidents to determine root cause and corrective actions?
RISK-09	Do you establish and maintain a security program that addresses risks from suppliers and third parties?
RISK-12	Have you implemented processes designed to ensure continued monitoring of supplier risk posture over time?
COMP-12	Do you have cybersecurity risk insurance? If yes, provide details (coverage, limits, exclusions).
COMP-13	Do you have dedicated information security staff responsible for ensuring compliance with applicable standards and regulations?

Table A.5: Example of requirements questionnaire

Appendix B

Interview

B.1 Transcript

Rui: Good afternoon, I am currently working on my master's thesis, which aims to assess the maturity of the cybersecurity risk management process in supply chains. At this stage of the work, I am validating the proposed model. Throughout the questions, if you have anything to add, or if you think something could be changed, or anything you find relevant, I would like you to provide your input. To give a bit of context about the scope of the work: it was identified that although there are frameworks on maturity, on cybersecurity, and on risk management in supply chains, there was a gap in bringing all these topics together. Therefore, the objective of this work is to fill that gap and present a maturity framework for the third-party cybersecurity risk management process. For the first question, I would like you to briefly introduce yourself, your experience, and your background within the topics of maturity, risk management, supply chains, everything you find relevant.

X: So, my name is X, and I am currently a coordinator in the area of GRC - governance, risk, and compliance - at a retail company in Portugal. I have around 10 years of experience. I started in a company focused on the energy sector, working on incident management, vulnerability management, identity management, audits, ISOs, and so on. In a second company, I was more focused on GDPR, ensuring compliance with the General Data Protection Regulation, oriented toward security assessment, privacy by design, privacy by default, and associated risks, taking into account the criticality of assets and applications. The controls that need to be ensured, versus the state of the art of those same systems, all aligned with privacy by design and privacy by default. Here, at the company where I currently work, I have been for 6–7 years now, coordinating this team and my area - governance, risk, and compliance. Governance is oriented toward the regulatory framework, based on ISO standards. We have a framework, which we call "security by design", although it could have another name, based on ISO 27001 and 27002. Then we include the control requirements necessary under GDPR, but focused on IT. They speak of ensuring confidentiality, integrity, and availability, and we interpret what that means at the IT level. We do not look at writing a privacy policy, that's for the legal side. Instead, we focus on more technological components, employee awareness, and so on. Then we have the risk component, where we assess

application risks and third-party risks, that is our main focus, strongly oriented toward security by design. But we adapt the controls we assess according to scope. For applications, we have a set of questions and requirements to evaluate. For third parties, we look at contractual matters, shared or non-shared responsibilities, the assets involved, personal data, and we already have a more tailored set of questions. Depending on whether they are compliant or not, that represents risks or nonconformities. We also monitor incidents that may be related to these partners, taking a risk-oriented view of the type of relationship this third party has with us, whether it concerns a critical asset of the organization or not, etc. Finally, the compliance component: for example, NIS2 was recently transposed, finally, and we assess what that represents for us and for our company. What is our scope? What are we required to comply with? My team has to interpret the law ourselves. We are a very transversal team that also looks at legislation, but always from an IT perspective, including audits. That's more or less it, across these three areas.

Rui: In terms of maturity more specifically, is there an approach to this topic?

X: Regarding maturity level, we are not an ISO-certified company, because it is not mandatory. It is a path we have been working on. However, in terms of maturity, we do have a set of controls. We do not follow a CMMI (Capability Maturity Model Integration) methodology, nor even the maturity model or the framework that the National Cybersecurity Center implemented relatively recently. But we do look at those references, even though we don't have an official process.

Rui: The purpose of this initial phase was to give a bit of context about your profile. I will now move on to the framework itself. Later, I will split this into slides so that the images appear larger and so we can discuss the framework in more detail, part by part. Going back a bit to the initial part of this research, in the background study on this specific topic, two main challenges were identified regarding the implementation of the framework: transparency and alignment of information. This is at a strategic level, both within organizations themselves, across different hierarchical levels, as well as between the various organizations in the supply chain. I would like to know, since you have experience in this area, what is your opinion about these challenges? Do you agree? Have you had any specific experiences related to this?

X: From the accountability point of view, right? Making it very clear. That is very important, having the attribution of what we call accountability, the "A" in the RACI matrix, and making it very clear what the role of each function is. Because this also helps to know where the process begins. I'll give an example of something we are currently dealing with internally: all third-party contracting must start with Legal. The need itself always comes from the business, from whoever owns that need—identifying, "OK, these are the players we want to contract", but Legal has the main role here to then guide and assess other risks.

Rui: I would perhaps like to make a distinction here between the internal part of the organization and between the different organizations. I assume when you mentioned Legal, you were referring to the process within the organization. What I want to understand here is whether you face any professional challenges in terms of communication and strategy alignment with third parties in this case?

X: My team does not need to have direct contact with third parties. That responsibility lies with the ownership—the contract owners, whether it is the business, IT, or another area. What we look at, and must look at, is the risk perspective. For example: this partner is very critical, and a risk assessment has never been performed, that's critical. Or, this partner now falls under the scope of NIS2, so a contractual review is necessary, with the addition of more technical and organizational measures. We have to raise these issues. But the direct contact should not be with us.

Rui: Ok, perfect. So now I'll talk a little more about the framework itself. Let's start from the beginning (switches slide). Here we have the first phase, which is called the pre-implementation phase. It consists of an initial awareness stage, where assets, stakeholders, maturity levels of the assets, risks, and consequences are all registered and taken into account. There is an identification step here. Then, when there is a decision to subcontract a service, the SCOR model is used. I don't know if you are familiar with what the SCOR model is, if not, I can give you a short explanation.

X: You can give me a short explanation, that's fine. Rui: The SCOR model is essentially a framework that aims to help organizations in decision-making. It helps us clearly structure the expected outcomes, the expected inputs as well, and the objective we want to achieve with this. What does this align with? Since we are talking about a third-party supply chain, having a structured decision-making model like this, even for communication between partners, makes the process much more efficient. So, at this stage, for implementing decision-making around subcontracting third parties, this is the first key point introduced into the framework. What I'd like to know is: what do you think about the impact of introducing this model at the moment of contracting? Positive or not?

X: So here you already have the listing of assets, right? And their classification. And then, depending on the need, whether to subcontract or not, you apply this SCOR model to help with the decision-making.

Rui: I just forgot to mention one thing. The goal is to actually evaluate maturity. And maturity is assessed according to different levels. Each level has sublevels, let's say, with a checklist for that level. For example, let's imagine we are at level 2 and there are three sublevels within that level. We want to achieve two more. These would be metrics entered into the SCOR modul, so the expected outcome is exactly to meet those two, with the aim of moving to level 3, 4, and so on.

X: So the maturity refers to that partner, that third party, for subcontracting that service?

Rui: No. The maturity is for the entire process itself, the overall supply chain cybersecurity risk management process.

X: Yes, yes, ok. Then we can move on to the next level. This seems good to me. I need to evaluate here. The asset is important, it's the foundation. Having awareness of the asset, its important, also helps the organization to set priorities. I have my team's focus priorities, and also a sense of needs and improvement areas. I agree with this.

Rui: So, after this pre-implementation phase with the model, there is then a decision to proceed with an acquisition, and we move on to the implementation phase (switches slide). The

implementation phase begins with an analysis stage. How does this analysis works? There is a request for tender issued by the organization that is subcontracting, which defines all the requirements whether organizational, location, budget, everything is pre-defined. Then the third parties respond to this request, and compliance with the requirements is evaluated, as well as the importance of the asset. Next, the type of relationship that can be established is determined based on this compliance with the tender requirements. That's why, when moving from the identification stage to the analysis stage, this evaluation is also carried out with what I introduce as part of my framework: the organization's maturity seals. These maturity seals range from bronze to gold. They evaluate more topics, but the ones I use here, the ones I considered most relevant, are the privacy level and the security level. These are the two seals taken into account for this work. We also consider the consequences of incidents, which come from the asset registry and feed directly into this stage. And then, based on the type of relationship to be established that is, the shared level of responsibility, the maturity seal, and the incident/consequence data, a new risk level is defined for this potential subcontracting. Then we move to the decision-making moment, considering all the evaluations of those who responded to the request for tender, and the organization makes its decision based on what it considers best. After that, there is a contract signing stage. I'd like to know your opinion, first of all, about the impact of these maturity seals. I don't know if this is something you work with, or take into account when contracting third parties. Do you think it could bring reassurance at the moment of contracting, in terms of transparency? And, of course, your general opinion on this topic.

X: That helps in large companies. So, you're assuming that the company you work for has enough budget to acquire services. In those cases, you may find maturity seals with third parties, but you won't find them everywhere. So, from our side, it's not a mandatory requirement, but we do look at whether they have certifications or not, and other criteria. But we don't make it mandatory to look at maturity seals, because unfortunately we still don't find them in many companies. But internally, I do include these issues, whether to look at the maturity seal or not, or at a set of requirements. And from what I understand of your process: we start with assets in the first phase, then we do an improvement analysis, a maturity model analysis, and so on. What type of third-party acquisition are we talking about here? Human resources?

Rui: Processes, services, anything within the cybersecurity domain.

X: Ok. Then we move on to the set of acquisition requirements, the Request for Tender. This is like a Request for Proposal, it's the same, at the end of the day it means the same thing. So, you're assuming there's a Procurement phase, a Search for Suppliers. Normally there's only one option, and that has to be it, in the real world. But yes, ideally, that's how it would be. The important thing is that there is an analysis, it's very important to define responsibilities, to really understand whether they are the owners, and whether we are going to have a high level of dependency on them or not. The point about the seals is what I already mentioned.

Rui: Then I'll just briefly touch on this part about contract signing. As an alternative to seals for suppliers that don't have them, what are the characteristics you look at?

X: We look at the seals, we have a set of requirements, and we check: compliant, not compliant, compliant, not compliant. And that then results in a measure.

Rui: So you already have a predefined checklist?

X: If it's certified in that area, yes. In that case, we don't need to look further. We assume everything is fine at that first stage. But if it's not, then we need to have an alternative.

Rui: The topic I mentioned earlier, transparency and alignment, I decided to address directly here in the contract signing stage. I introduce the subject of audits as a way to address this. But, of course, there are no perfect solutions, and even within audits problems were found. One issue identified is audit fatigue. That is, if audits are carried out constantly, if we want to always be on top of everything, it creates audit fatigue, and so it's not a perfect solution. Then we also have the internal aspect: the more people are aware that many audits are happening, the more they tend to take riskier actions, let's say, more from the human side, whether because they think all controls are up to date, and everything will be fine. It creates a false sense of security. So, to address audit fatigue, this is decided at the time of contracting. In an ideal world, for each asset, all organizations in the chain related to that asset would share a common external auditor, but we all know that's not feasible. Therefore, at the moment of contracting, the decision is made on external audits and the timelines that the organizations agree on. And to counter the riskier behaviors that may arise from more audits, the concept of risk compensation is introduced. That is, compensating for risk-taking behaviors critical actions, whether from IT, Lead Teams, or others. For example, a critical action must always be approved by management. In other words, security controls are applied for critical high-risk actions, to avoid these loopholes caused by the false sense of security. So, what I'd like to know is, maybe you're not deeply into audit topics, but I'd like your opinion on how to tackle both transparency of information and strategic alignment.

X: So, what do I gather here? We have the need, the requirements, and we already have a selection of partners, the third parties that will provide the service, and we carry out this analysis. In this analysis, we choose a partner to contract with, and in the contract we address the issue of audit fatigue. What have we observed? One of the things we always look at is what is contractually established. Beyond our assessment of the partner, we require that the contract includes what we call TOMs, technical and organizational measures, and contractual clauses from an information security perspective. And one of those clauses is the obligation for audits. We can audit the partner whenever necessary, with X days' prior notice, etc. So that is established in the contract. That is the point we can address at the time of contracting. And then, regarding the audits themselves, we are aware of audit fatigue. What we do, and are moving towards, is this: if a partner has many security risks, or has already had one or two critical incidents in a year, then they must be audited. We make use of that clause. It's a measure we have, based on the third party's level of criticality and the incidents they've had, which then triggers our response. Or, for example, we send a questionnaire, imagine, all critical partners automatically receive a questionnaire annually to check if the measures, the security level, the seal, are still valid, and whether they still apply. Or, in other cases, we perform audits, to see if that partner is really behaving poorly. But we don't

do audits at the very beginning. At the start, we just make it clear that they are possible. When we're doing the analysis, we try not to be too exhaustive, because we don't want to turn it into an audit. We are already asking for evidence, and that alone is a lot of effort. Meanwhile, the teams want to contract that service to start using it. So, the analysis is carried out, and then we provide an opinion. But we ensure that audits, and everything else, are clearly established in the contract.

Rui: Just to make sure I understood, there is a periodicity, and unless there is a specific reason that triggers an audit, or a request before that period, the period established contractually is always respected?

X: Yes, yes. It's not exactly a strict period. Well, it is a period. Annually, for example, there may be a clause stating that the organization can audit, may want to audit the partner, and must inform them X days in advance.

Rui: Ok, what I wanted to clarify is that it's not an obligation, it's a possibility...

X: Yes, and then what does that involve? It involves budget, money, hiring auditors to audit the partners, or having dedicated internal teams, people's time. So, there are a set of factors. That's why it's a criticality-based analysis. The clause exists and gives us the authority to audit, but we only actually audit if we consider it relevant. The questionnaires, those are more like informal audits.

Rui: Yes, exactly. To counter the fatigue I mentioned earlier.

X: For example, I can give concrete examples: we don't yet audit partners directly, but we constantly monitor more critical partners. However, we do have partners who audit us, because we also provide some services to them. They send us an annual assessment, a form we have a certain time to complete, showing evidence. That's not really an audit, because the partner doesn't come here in person, except in special cases. But we don't do that to them. Still, it's something that is established contractually, depending on the type of contract and the need.

Rui: So, after the contract signing, we arrive at the final part of the work, which is the improvement phase, where maturity is effectively reassessed against the established metrics. To give some context: in this work, six levels are defined, each level with a certain number of sublevels. The reassessment is made against the metrics of these sublevels, like a checklist to evaluate the maturity level. As I said, it's evaluated against the metrics, then improvement areas are defined. In other words, since you won't usually reach the first time, or in many cases won't reach, the ideal level of maturity, already in this improvement phase areas are defined where improvement is still needed, where adjustments are still required. Within these, a set of initiatives is selected. What are these initiatives for? To return to the SCOR model, because it helps us update the SCOR model context, where the inputs and outputs are defined, and what we can improve in the short, medium, and long term. We then build a kind of timeline, to guide the organization on how and why to improve. So that, at the final moment, when reviewing the maturity level at the end of the framework, we can reach the target maturity level of the organization. What I want to ask is this: maturity in this context, within the scope of this work, aims to evaluate or improve the structure of the risk management assessment process, as I mentioned earlier, the agility in communication between

stakeholders addressing the problem of transparency and alignment, as well as the trust between them, which is important, and to improve resilience against cybersecurity incidents. So, now that I've given you an overview of the framework as a whole, I'd like to get your input, suggestions, changes, improvements, opinions.

X: So, let me recap the process to check that I understand it correctly. For example, let's say we have a critical business asset. I carry out a maturity analysis. We see that it has many security weaknesses and needs, say, a pentest. So, the maturity level and the need are identified, and then we launch a request for tender and look for partners to carry out this pentest. So, we sign the contract, carry out the pentest, and then we reassess the asset's maturity and see: ok, we actually performed actions through this acquisition to ensure the security of the systems. What do I see here? I see that, ok, we evaluate the maturity level of the asset, and then what we do to improve that maturity level, or the maturity level of the organization, can take several forms. It could be internal training, dedicating internal teams' time to training. It could be creating a new team if existing ones can't respond to the need. Or it could be subcontracting an external service to bring in expertise. In other words, the process here is to address this reduced capability in the process. Yes, this makes sense to me. I see this model as being very oriented toward internal controls, an internal controls area where, ok, I assess and control these processes. In ISO, it's the SOA, the Statement of Applicability, which companies then use for internal control, where it is necessary to carry out a maturity assessment. And yes, this is a decision, subcontracting a service. I totally agree, we do this frequently, not only for software, not only for people, but also for knowledge, for consulting, for example, to improve something. Yes, it seems good to me. But it seems that something is missing, the path from contract signing to execution. Before you can reassess maturity, you have to execute that contract, that contractual relationship, and then see the results. That is the way to see improvements in the weakness, in the improvement action we identified, because we can only assess after actually executing some action.

Rui: I could talk about the use case, but everything you mentioned aligns with it. I'll talk here about a stage, which is what I discuss in the use case: the actual assessment. That is, when it moves from conceptualization to action. In the use case I say, for example, after six months, after three months, there is a concrete evaluation. Because at the start everything is registered against the benefit, but then it's actually about how things happen. And the goal of this improvement phase is for it to be continuous. That is, ok, we have the evaluation against metrics at the conceptual stage, after the contract signing, but these metrics will be under continuous evaluation. So, in action, it is continuously assessed, after three months, six months, nine months, and so on.

X: Ok, so we want this contract, this service for X, and to periodically assess. Yes, I agree, I think that's the only part that's a little less clear, but everything else is fine.

Rui: I just have a question. Earlier you mentioned it being more oriented toward internal controls. With the metrics, everything you said is correct and aligns with many of the elements I have in the metrics, which I found interesting. For external controls, I'd like your opinion. What I talk about is those joint exercises, those simulations, let's say for example, pentesting, running

attack simulations, so these joint exercises between organizations with the aim of moving from conceptualization to action. I'd like to know your opinion on this inter-organizational aspect, not so much internally, what do you think?

X: There is starting to be some support between entities, but not much yet. What exists, for example, is work within a group. So, from time to time, we gather all the companies in the group and work together to improve processes, to discuss things. That happens. One of the things that NIS2, the National Cybersecurity Center, and even ENISA now emphasize is also the sharing of vulnerabilities. If one entity discovers a vulnerability, sharing it with others so we can all learn from it. It's complex, because of competition, let's say. But on the other hand, the National Cybersecurity Center has been encouraging this information sharing, centralizing everything with them. The reports they produce, the risk observatory and so on, are based on information they receive from other companies. If one company has a vulnerability in a system, they already know which other companies use that system and share that same information with IOCs and so on. So, in the end, the National Center is the central hub for this type of information. Something that is important, and that we would like to have if the National Center could promote it, is a pre-assessment of partners. For example, we know that our IT sometimes cannot meet all needs. So, there's a specific external partner that helps us develop many things. We know that partner is trustworthy, develops according to our premises, and so on. Our idea would be to have that same visibility of partners that are recommendable. Other companies have already subcontracted them and recommend them, confirming that from a security perspective they are fine.

Rui: I think that's somewhat aligned with the maturity seals that come from the National Cybersecurity Center. They evaluate across four categories, if I'm not mistaken. Each category has a seal, and then there is an overall seal. Well, that's everything from my end thank you so much for your time.