What criteria can best support Austrian companies in the secure procurement of IT systems?

Master Thesis

For attainment of the academic degree of
Master of Science in Engineering (MSc)

in the Master Programme Cyber Security and Resilience
at St. Pölten University of Applied Sciences

by
Eric Schinwald
cr211513

Advisor: FH-Prof. Mag. Dr. Simon Tjoa

St. Pölten, 07.06.2023

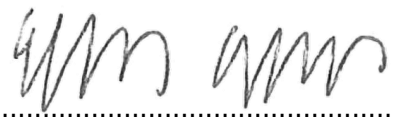
Declaration

I hereby affirm that

- I have written this thesis independently, that I have not used any sources or aids other than those indicated, and that I have not made use of any unauthorised assistance.
- I have not previously submitted this thesis topic to an assessor, either in Austria or abroad, for evaluation or as an examination paper in any form.
- This thesis corresponds to the thesis assessed by the assessor.

St. Pölten, 07.06.2023 .....

Place, Date



.....

Signature

Acknowledgements

I would like to express my deepest appreciation to FH-Prof. Mag. Dr. Simon Tjoa for his support in writing this thesis. This thesis would not have been possible, without his insights and feedback,

Thanks also to my girlfriend Rachael who proofread my work and encouraged me every step of the way.

I would also like to thank my parents for enabling me to study cyber security.

Lastly, I would like to thank my interview partners Thomas Kerbl and Erik Rusek for taking time out of their days to engage with a cyber security student for his thesis.

Abstract

Currently, attacks through the supply chain are on the rise. Therefore, businesses need to vastly improve their procurement processes in terms of cyber security or be faced with catastrophic incidents. This master thesis aims to offer guidance for Austrian companies on secure procurement practices. It does so by showing aspects of current and future legal obligations and by extracting criteria from well-known standards and guidelines that can be used to improve the procurement process. The secure procurement criteria are then evaluated against criteria from experts on secure procurement. By the end of the thesis a procuring business should have a clear idea on how to conduct secure procurement and what practices are essential.

Kurzfassung

Aktuell nehmen Angriffe durch die Lieferkette stark zu. Deshalb müssen Unternehmen Sicherheitsthemen in ihre Beschaffungsprozesse besser miteinbeziehen oder sie laufen Gefahr, katastrophalen Vorfällen ausgeliefert zu sein. Diese Masterarbeit zielt darauf ab, einen Leitfaden für österreichische Unternehmen darzustellen. Sie tut dies, indem Aspekte von aktuellen und zukünftigen gesetzlichen Regularien analysiert werden. Außerdem werden Kriterien von anerkannten Standards und Handbüchern extrahiert, mit dem Ziel, Beschaffungsprozesse zu verbessern. Diese Kriterien der sicheren Beschaffung werden dann mit Hilfe von Experten evaluiert. Am Ende dieser Masterarbeit sollte ein beschaffendes Unternehmen eine klare Idee haben, wie sichere Beschaffung praktiziert werden kann und welche Aktivitäten essenziell sind.

Table of Content

1 Introduction

As of 07.06.2023, MOVEit is the latest in a series of businesses suffering from supply chain attacks with widespread negative effects. Here, a vulnerability in MOVEit Transfer [1] was used to gain unauthorised access to sensitive data of a plethora of small and large businesses that have procured said software [2]. As this attack shows, many businesses, large and small, are not sufficiently prepared for attacks stemming from procured products and services.

While some large international corporations have the resources to define and develop their own secure procurement processes, smaller businesses often do not have such luxury and have to rely on public publications about secure procurement. Many different publications exist but only a few have been adapted to the European or even Austrian market. That is an area of research that is still in active development.

Therefore, it is necessary to define criteria that are tailored towards Austrian companies practicing secure procurement. This thesis is the attempt at delivering a possible solution for this problem.

First, the thesis will disclose the methods that were used for identifying, analysing, and evaluating the literature that the criteria are derived from. Next, is a section that delves into the current and future legal obligations for Austrian businesses. Thirdly, the previously identified literature will be evaluated, and criteria will be derived. To review the created criteria, an empirical evaluation in form of an interview will take place. Lastly, the thesis will be concluded, and a future outlook given.

2 Methods

In this section, several methods are presented that have been used for the identification and evaluation of publications and the criteria described in those publications. Some of the methods includes a customised workflow of PRISMA 2020 and the definition of exclusion and inclusion criteria for publications. The section will also cover, how criteria are extracted in the literature evaluation section.

2.1 Research methods

2.1.1 What is PRISMA 2020

The PRISMA 2020 Statement is a set of guidelines that are designed to support systematic reviews of studies in the health sector. The two major parts of the statement document consist of a flow diagram template that defines a clear method for systematic review as well as a checklist that details reporting recommendations [3].

While the PRISMA 2020 Statement's intended purpose is for a systematic review of healthcare studies, it is also applicable for much other scientific research when slightly modified.

2.1.2 Custom Workflow

As mentioned earlier, our usage for PRISMA 2020 differs from the intended usage. We used the core workflow from PRISMA 2020 to structure our research and facilitate a structured review but adapted and simplified the workflow where it was necessary. In total, 82 works were analysed with the custom PRISMA 2020 workflow.

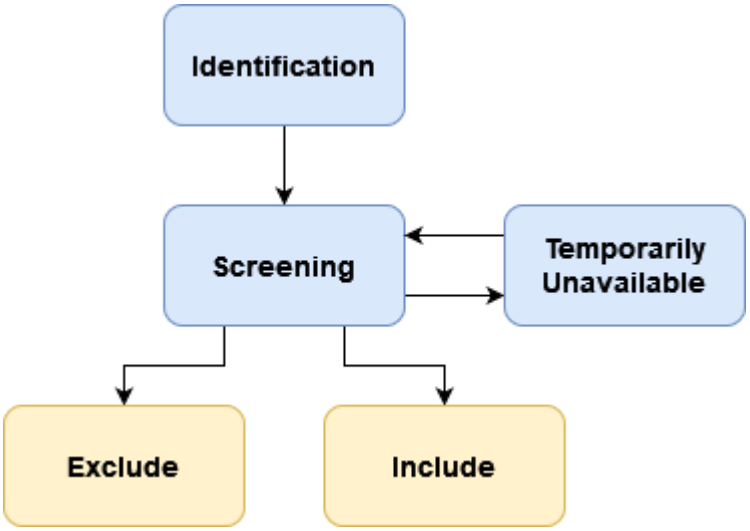


Figure 1 Custom Research Workflow

Identification:

All publications first complete the identification process. Here, the publication will be searched for references to other works related to secure IT procurement. After this step each publication will move on to the Screening process.

Screening:

First, each publication in this process is being attempted to be retrieved. If this is not possible, the publication will directly land in the “Excluded process” where the cause will be documented. The next step is to summarize the Abstract, Introduction and Conclusion of the publication. Furthermore, an analysis based on the research criteria in section 5 is conducted. From this analysis it is decided whether the publication will be excluded from the thesis or whether the work will be included and used. The entire decision process is documented as part of the analysis.

Temporarily Unavailable:

Whenever a publication is not available the moment it was first attempted to be retrieved it will become part of this process. Most common causes for this are technical issues or acquisition cost. Critical here is that this is temporary and will likely be resolved in the future. If this turns out to not be true, the publication will move to the excluded process.

Included:

All publications here have successfully completed all stages beforehand. This means that all publications here are of adequate or high quality and fulfil the research criteria we have defined at the start of the research process.

Excluded:

All publications that land in this process will not be used in any shape or form by the master thesis. The reason for exclusion will be documented and the publication is archived.

2.1.3 Research Criteria

2.1.3.1 Research inclusion Criteria

We have determined the following qualitative criteria to be useful when selecting publications for our master thesis:

- Relevancy to the research question
- Usefulness for Literary Evaluation
- Usefulness for Introduction section

2.1.3.2 Research exclusion Criteria

We have determined the following criteria filter out the largest amount of unwanted works without being too broad:

- Unavailability
- Budgetary constraints
- Not relevant enough to the research question
- Outdated
- Poor Quality

2.1.4 Sources

As recommended by PRISMA 2020, we have selected the following sources in advance. We, however, also allowed for publications from other sources but have not actively searched those for relevant works.

- IEEE
- ISO/IEC
- Springer Verlag
- BSI
- Austrian government agencies
- NIST

2.2 Literature evaluation methods

24 publications were summarised and evaluated for criteria of secure procurement. Only parts relevant to secure procurement were extracted and documented in origin tables in Appendix A, where the origin of each criterion is recorded. Often, similar criteria are recommended in several independent documents. All those cases have also been recorded in the origin tables.

3 Legal Obligations

This section will look at legal obligations through the lens of IT procurement. While some of the laws analysed here cover a large area of content, the only ones explored here are the parts that are relevant to secure IT procurement. This section is not meant to be a comprehensive overview of all possible legal obligations for procurement processes, but it should aid as a guide to what forms legal obligations can take.

3.1 Current Legal Requirements

This subsection will discuss several pieces of legislation that are or have been in effect in the European Union or on the North American Continent.

3.1.1 GDPR

The main goal of the General Data Protection Regulation (GDPR) is to protect the rights and freedoms in the personal data of natural persons. The protection comes from laying out rules for processing personal data [4].

The GDPR dictates that all collected personal data must be relevant, limited, accurate and processed lawfully, transparently and securely. Generally, processing is deemed lawful when the data subject, the natural person, whose personal data is processed, explicitly agrees to the processing for a specific purpose. There are, however, several exceptions for that rule. For instance, to comply with other legal requirements or for a task carried out in the public interest [4].

Natural persons also get a considerable number of rights under the GDPR explicitly [4]:

- “Right of access by the data subject”
- “Right to erasure”
- “Right to restriction of processing”
- “Right to data portability”
- “Right to object”
- “Right to rectification”
- “Right to be informed”

- “Right not to be subject to a decision based solely on automated processing”

Besides the data subject, two more distinct entities exist: The controller and the processor. The controller is responsible for implementing appropriate technical and organisational measures to ensure the rights of natural persons during processing. If the processing is to be carried out by a processor, the controller must verify that the processor possesses the ability to implement technical and organisational measures to ensure the rights of natural persons [4].

Failing to comply with any of the GDPR rules and regulations can lead to significant compensations and/or fines for businesses until the violation has been resolved [4].

The GDPR applies to any controller or processor residing in the European Union, regardless of where the processing takes place. The regulation also applies whenever personal data from natural persons in the European Union is processed by non-EU controllers or processors [4].

The GDPR also elaborates on several critical security aspects of data processing. Personal data must be pseudonymised and encrypted wherever possible, accessibility needs to be restored within a reasonable timeframe after an incident, a process needs to be in place that regularly tests the effectiveness of organisational and technical measures, and ongoing confidentiality, availability and integrity must be ensured while taking into account the technological state of the art, the cost of implementation and the risks to the rights of natural persons [4].

The last measure also sets requirements for the controller and processor to take extra care when procuring products and services from third parties. Procured hardware needs to be verified for the further technical and organisational measures to function as intended. Procured software needs to be verified so that there is a minimal risk of information leaks and integrity compromise to the personal data of natural persons [4].

There are many other aspects of the GDPR exist, but these go outside of the scope of this research [4].

3.1.2 NIS Directive

The NIS directive is a piece of legislation in the European Union that came into effect on the 8th of August 2016 and aims to achieve a high level of security of essential services within the European Union [5].

Each member state of the European Union must identify providers of essential services that belong to certain industries. These industries include: Energy, Transport, Banking, Financial Market Infrastructures, Health Sector, Drinking Water and Digital Infrastructure. Whether or not a business is deemed a provider of essential services within those sectors is determined by each member state based on three criteria [5]:

> "(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
>
> (b) the provision of that service depends on network and information systems; and
>
> (c) an incident would have significant disruptive effects on the provision of that service."

At a minimum the following factors must be taken into consideration when determining what a significant disruptive effect would be [5]:

> "(a) the number of users relying on the service provided by the entity concerned;
>
> (b) the dependency of other sectors referred to in Annex II on the service provided by that entity;
>
> (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
>
> (d) the market share of that entity;
>
> (e) the geographic spread with regard to the area that could be affected by an incident;
>
> (f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service."

If a business is deemed a provider of an essential service, certain requirements for security and incident notification come into effect. Member states must ensure that providers of essential services manage risks regarding the security of the network and information systems, using appropriate measures. Furthermore, member states shall require operators of essential services to implement measures to minimize the impact of network and information security incidents. Member states must also enforce that operators of essential services notify the competent

authority of incidents that have a significant disruptive effect. These requirements for operators of critical services also play a big part in IT procurement in terms of risk management, notification requirements and mitigation, among other things. Therefore, IT procurement processes must adapt to establish compliance with these requirements [5].

For member states to fulfil their duties as laid out in the NIS directive certain documentation needs to exist and be provided upon request. Firstly, all operators of essential services must be able to provide information to assess the network and information security of the company. Secondly, any proof of correct and effective implementation of security policies must also be made available. For the IT procurement processes, this means documentation about the acquisition and operation of procured goods and services needs to be collected as part of the reporting duties [5].

The NIS directive also lays out requirements specifically for three types of digital service providers: Online marketplaces, online search engines, and cloud computing services. The requirements set out for digital service providers are similar to the requirements set out for operators of essential services. However, the elements that member states of the European Union must consider are more clearly and explicitly defined [5]:

> “(a) the security of systems and facilities;
>
> (b) incident handling;
>
> (c) business continuity management;
>
> (d) monitoring, auditing and testing;
>
> (e) compliance with international standards.”

The NIS directive has been repealed through the introduction of the NIS2 directive in January 2023.

3.1.3 NIS2 Directive

The NIS2 directive is an EU directive that came into effect on the 16th of January 2023. Currently, EU member states are in the process of adopting the directive into their respective laws. The goal of this directive is to implement a high level of cyber security across the European Union. It achieves this by setting out requirements for national cyber security strategies, risk-management measures and rules and obligations for essential and important entities.

The following list of definitions spell out what entities are considered essential entities under the NIS2 directive [6]:

> “(a) entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC;
>
> (b) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
>
> (c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;
>
> (d) public administration entities referred to in Article 2(2), point (f)(i);
>
> (e) any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);
>
> (f) entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive;
>
> (g) if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.”

Any entities that are defined in Annex I or II of the directive but do not fall under the previously mentioned definition for essential entities, are deemed important entities [6].

Regardless of which classification, both important and essential entities will be required by EU member states to take technical, operational and organisational measures to manage cyber security risks and mitigate the impact of incidents to the service. The required measures include but are not limited to [3]:

> “(a) policies on risk analysis and information system security;
>
> (b) incident handling;
>
> (c) business continuity, such as backup management and disaster recovery, and crisis management;

> (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
>
> (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
>
> (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
>
> (g) basic cyber hygiene practices and cybersecurity training; (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
>
> (i) human resources security, access control policies and asset management;
>
> (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.“

Point (d) is especially relevant for procurement as it enforces the proper management of supplier relationships by entities like the procurement department.

An important factor here is that the management bodies of essential and important entities specifically can be held liable by an EU member state if implementations of these measures are not conducted properly [6].

Both important and essential entities are required to notify either the computer security incident response team (CSIRT) or its competent authority of the respective EU member state in case of an incident with a significant impact on their service within tight time limits. If appropriate, those entities must also notify the recipient of their services of the significant incident and communicate any measures or remedies than can be taken as a response to the incident [6].

What defines a significant incident is clearly outlined within the NIS2 directive [6]:

> “(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
>
> (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.”

One of the major differences between the NIS2 directive compared to the previous NIS directive is the establishment of a European vulnerability database [5], [6]. The vulnerability database will be coordinated by each member state's designated CSIRT to ensure that entities concerned can be identified and contacted, persons reporting a vulnerability are assisted and vulnerabilities that affect multiple entities are managed. The European agency ENISA must develop and maintain a database for these reported vulnerabilities. Procurement departments of essential and important entities then can use this vulnerability database in their IT procurement decisions [6].

The NIS2 directive came into effect on the 16th of January 2023. This means that EU member states now have until the 17th of October 2024 to implement the measures as laid out by the NIS2 directive. Businesses, and their respective procurement departments, have until this date to implement their own measures to comply with legislation from those EU member states.

3.1.4 NERC CIP-013-1

NERC is the North American Electric Reliability Corporation. Among other things, NERC develops mandatory reliability standards for the North American bulk power system. The reliability standards cover a wide array of topics such as Design, Maintenance, or Critical Infrastructure Protection. Each of these topics contain dozens of individual standards that operators of bulk power systems must comply with. NERC also requires a CIP Senior Manager that manages compliance with all standards under Critical Infrastructure Protection [7].

One such standard that relates to secure IT procurement would be CIP-013-1 Cyber Security – Supply Chain Risk Management. This standard defines controls for supply chain risk management to mitigate cybersecurity risks. It is structured into an Introduction section, a requirements and measures section, and a compliance section. Furthermore, it defines and describes levels of violation severity levels from low to severe [7].

The standard requires each responsible entity to develop and use a supply chain security risk management plan that covers, among other things, identification of security risk from vendor systems, disclosure by vendors of known vulnerabilities and verification of software integrity and authenticity [7].

Another important part of CIP-013-1 is that the fulfilment of these requirements needs to be well documented, which includes planning documents but also working documents, so it is demonstrated that required plans are in fact in use. All evidence

needs to be retained at least three calendar years or longer if an investigation is in progress [7].

As mentioned earlier, CIP-013-1 was created by NERC which is only responsible for standards that North American bulk power systems operators fall under. European companies generally do not have to comply with this standard. However, CIP-013-1 is an excellent example for an industry specific standard. Plenty of industry specific standards exist for European energy providers and operators as well [7].

3.2 Possible Future Legal Requirements

This subsection will discuss two major European acts that are currently in the proposal stage but are likely to come into effect after passing a vote.

3.2.1 Cyber Resilience act

The Cyber Resilience act is a proposed regulation that lays down rules and essential cybersecurity requirements for the development of products that contain digital elements with connection to a device or network. The regulation also sets out requirements for the vulnerability handling processes for manufacturers and economic operators. Like the GDPR, companies that either reside in the European Union or deliver to customers from European Union member states must abide by these rules [[8].

The cybersecurity requirements that all manufactures of products with digital elements must follow are as follows [8]:

> “(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;
>
> (2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;
>
> (3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:
>
> (a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial-of-service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users."

The manufacturer must perform a conformity assessment of all products with digital elements to assess whether all these essential requirements are being met. Depending on how critical the product is, it may also be required to have a 3rd party certify that all the essential cybersecurity requirements are fulfilled instead of an internal process [[8].

According to the regulation, manufacturers also must exercise due diligence when integrating components from third parties to ensure that products with digital elements contain no known vulnerabilities. This is where secure IT procurement processes become vital [8].

3.2.2 Artificial Intelligence Act

The Artificial Intelligence Act is a proposed EU regulation that harmonizes rules for placing, importing, and using artificial intelligence systems within the European Union. The act lays out rules for three different categories of AI systems: Prohibited, Low-risk, and high-risk systems [9].

The following practices are generally prohibited under the proposed Artificial Intelligence Act [9]:

> "(a)the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;
>
> (b)the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;
>
> (c)the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:
>
> (i)detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
>
> (ii)detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity; "

Setting restrictions on the use of AI systems means that during procurement, prohibited Artificial Intelligence practices need to be rejected as part of the process.

Furthermore, if an Artificial Intelligence System is deemed high-risk even more restrictions are enforced on placing on the market, putting into service or using the AI system in question. An Artificial Intelligence System needs to fulfil the following two conditions to be deemed high-risk [9]:

> "(a)the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;
>
> (b)the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II."

Furthermore, any product as mentioned in Annex III is classified as high-risk. Those products will not be described here, as Annex III can be expanded by the European Commission when necessary.

If a high-risk AI System is being acquired, the procurer must ensure that the following special requirements [9] are also factored into the purchasing decision and can be fulfilled:

- The instructions by the provider need to be followed, especially when it comes to human oversight.
- Input data needs to relevant for the intended purpose of the high-risk AI system.
- The high-risk AI system needs to be monitored and the provider needs to be notified if a risk or an incident occurs.
- Logs that high-risk AI systems generate shall be kept.
- The GDPR Regulation must also be followed and factored in when acquiring a high-risk AI system.

In the future, it is likely that harmonised standards will exist that will aid greatly in the procurement process. Any high-risk Artificial Intelligence System is presumed to be in conformity with the AI act if it adheres to a standard that is published in the Official Journal of the European Union [9].

To summarize, acquiring an Artificial Intelligence System or a high-risk Artificial Intelligence System, is likely to increase in effort once Acts like the Artificial

Intelligence Act come into effect. The procurement process of a company will therefore also have to adapt to the increase in requirements.

3.3 Overview for the legal obligations for a typical Austrian organisation

Table 1 Legal obligations stemming from regulations

	GDPR	NIS	NIS2	NERC	Cyber Resilience Act	AI Act
Always applicable	x					
Applicable depending on main business		x	x	x	x	
Applicable depending on the type of procured product						x
Reporting requirements			x	x		
Documentation Requirements	x	x	x	x	x	x
Risk management requirement			x	x		
Incident handling requirements		x	x			
Distinction between levels of criticality		x	x			x
Vulnerability management requirements		x		x	x	x

Table 1 shows the extracted legal obligations that arise from the different directives and regulations. Each “x” indicates where the legal obligation stems from. So, it is possible for a legal obligation to be enforced by multiple regulations.

4 Literature Evaluation

This section will focus on evaluating literature on secure procurement. Each publication is analysed through the lens of secure procurement. The publications range from strict standards to general guidelines in IT procurement. A few publications also offer advice on very specialised topics that also contain advice that can be used for general secure procurement. From the evaluations, criteria will later be extracted.

4.1 IT Grundschutz Kompendium

The IT Grundschutz Kompendium is an overarching set of requirements that aims to offer guidance on all areas of IT security. While the publication offers a wide area of very detailed documentation about cybersecurity, secure procurement is most covered as technical requirements for individual types of products.

The types of requirements recommended vary greatly, depending on the type of product. Some requirements are shared across different types [10, p. 717], [10, p. 802], [10, p. 812], [10, p. 828]:

- Requirements list
- Incident response plans
- Training
- Security policy
- Implementation plans
- Vulnerability management
- Maintenance

The Grundschutz Kompendium also contains a section that deals with the usage of cloud services [10, p. 295]. This section can used for guidance on the secure procurement of those types of services.

While not exhaustive, this publication offers a starting point from which secure procurement can be practiced. More in-depth guidelines and handbooks are needed to implement a full procurement process.

4.2 NIST SP 800-161r1

This publication is a 2022 collection of guidelines on how to identify, assess, and mitigate cybersecurity risks stemming from the supply chain. It achieves this by combining risk management activities with cybersecurity supply chain risk management (C-SCRM).

Integrating the C-SCRM process into the risk management process designed after NIST SP 800-39 [11] involves all three levels of risk management: The enterprise-level, the mission and business process level, and the operational level.

In level 1, the enterprise level, the overall C-SCRM strategy, C-SCRM policy and implementation plan are defined. Furthermore, the governance structure of the enterprise is set in respect to C-SCRM, so that leaders and executives can collaborate, delegate, make decisions, and prioritize resource allocations accordingly. Activities in this level also help to increase the consistency of mitigation strategies in respect to the strategic goals and objectives of the company in general. The main goal of these activities is to provide context to the entire company's mission and business processes that manage cyber security risks that are related to the supply chain. The responsibilities and accountabilities for these activities in level 1 generally lie with the C-level Executives of the companies. Level 2, the Mission and Business process level, further refines the strategy, policies, and implementation plan.

In Level 2, the general strategy, policies, and implementation plans from level 1 are used to create process specific plans. Each mission and business process is also met with the company's C-SCRM goals and requirements. Specific requirements are defined and overseen for the C-SCRM, including cost, schedule, performance, security, and several critical non-functional requirements.

The responsibilities for the activities in level 2 generally lie with business management of the company. This includes project managers, acquisition and supplier relationship management, research and development, and engineering. The supervisors for specific missions and business processes develop implementation plans that adhere to the plan laid out in level 1. The implementation plans created at level 2 then contain a more detailed plan on using the C-SCRM at the operational level.

The outputs of level 2 are then used in level 3 to apply the implementation plans from level 2 in the context of individual systems. Furthermore, the outputs of level 2 should also influence level 1 in an iterative manner for continuous improvement.

Level 3, the operational level, applies the C-SCRM to all personnel within the enterprise that is accountable for operational activities. That also includes personnel handling procurement. The main activities in this level engage with operational level risks arising from IT products and services acquired from the supply chain. As a first step, risk assessments are conducted that evaluate the likelihood and impact of supply chain threats. From this assessment a C-SCRM plan can be developed for each system that contains “information on the system, its categorization, operational status, related agreements, architecture, critical system personnel, related laws, regulations, policies, and contingency plan” [12]. Appropriately adapted controls are also part of each C-SCRM plan. Like the previous level, information gained from level 3 should iteratively aid in improving level 1 and level 2.

In order to successfully manage risks stemming from the supply chain, it is vital for C-SCRM considerations to be part of every step of the procurement life cycle process.

A crucial first step is to make sure that all supplier relationships are accounted for. There should be a central place where all information of relationships, contracts and products and services in use are gathered. Furthermore, each supplier relationship should be assessed and categorised depending on the criticality of the relationship. Further analysis on the supply chain risks is only possible after this step.

For each possible future supplier, C-SCRM requirements have to be checked for conformance and C-SCRM risks stemming from a supplier have to be identified and analysed. Even after a supplier relationship is already established, the conformity contractual obligations by the supplier need to be continuously verified and monitored. Monitoring is also necessary for any upcoming cybersecurity risks that did not exists at the start of the relationship.

Further complications arise when products and services are not exclusively acquired through the procurement department such as open-source software. This edge case also needs to be factored in.

The risk management of the acquisition process should also be reflected as part of the C-SCRM Strategy and the C-SCRM Implementation plan. Specific activities that constitute to such risk management include:

> “• Promoting awareness and communicating C-SCRM expectations as part of supplier relationship management efforts

• Establishing a checklist of acquisition security requirements that must be completed as part of procurement requests to ensure that necessary provision and protections are in place

• Leveraging an external shared service provider or utilizing the C-SCRM PMO to provide supplier, product, and/or service assessment activities as a shared service to other internal processes, including acquisition

• Conducting due diligence to inform determinations about a bidder's responsibility and to identify and assess bidders' risk posture or risk associated with a given product or service

• Obtaining open-source software from vetted and approved libraries

• Including C-SCRM criteria in source selection evaluations

• Establishing and referencing a list of prohibited suppliers, if appropriate, per applicable regulatory and legal references

• Establishing and procuring from an approved products list or list of preferred or qualified suppliers who have demonstrated conformance with the enterprise's security requirements through a rigorous process defined by the enterprise or another acceptable qualified list program activity [CISA SCRM WG3]

• Ensuring that products, including software or logic-bearing products (i.e., hardware), are supplied with a software bill of materials that complies with appropriate agency-approved protocols" [12]

All of these C-SCRM aforementioned activities take time. Therefore, leaders of the company need to allocate ample time and funding for these crucial activities. This ensures that results can be achieved without compromising on other requirements.

In order for an enterprise to be able to access information that is crucial to handling cyber security risks stemming from the supply chain, an information-sharing process with respective activities should be implemented. This information-sharing process not only takes place internally but also externally with information-sharing agreements with industry partners. Through sharing supply chain risk information, a collective understanding of the threats can be achieved that would not be possible with an individual company's resources. It also helps to detect active malicious campaigns against an entire industry sector.

Many personnel, especially at the operational level is crucial for the success of the C-SCRM and the procurement process. Each person has duties in managing

cybersecurity risk stemming from the supply chain. To successfully fulfil their duties an appropriate level of training, tailored to the specific position and responsibilities of the person, should take place. The requirements for the training should incorporated into all three levels of supply risk management.

For an effective C-SCRM program, an ongoing measurement of and reflection on the program is necessary. Companies can use several, well established methods to accomplish this task:

> "• Using a framework, such as NIST CSF to assess their C-SCRM capabilities
>
> • Measuring the progress of their C-SCRM initiatives toward completion
>
> • Measuring the performance of their C-SCRM initiatives toward desired outcomes" [12, p. 49]

All methods rely on information collection, analysis and reporting activities. This is another reason why the implementation of information sharing processes and activities is crucial for the success of the C-SCRM processes. Ideally, metrics are developed with the following development process.

Stakeholder Interest Identification in this step we identify all the different stakeholders and define their requirements depending on context needs for each stakeholder.

Goals and Objective Definition Here, the business identifies all performance goals and objective of the C-SCRM processes.

C-SCRM Policies, Guidelines and Procedure Review In this step all wanted policies, guidelines and procedures are defined are used to implement the C-SCRM.

C-SCRM Program Implementation Review All existing data and evidence is collected from which insights could be drawn.

Level of Implementation Here, measures are mapped to the previously identified Policies, Guidelines and Procedures to see the implementation progress of the C-SCRM program.

C-SCRM Program Results on Efficiency and Effectiveness In this step any measures that specifically measure the C-SCRM program's efficiency and effectiveness of the strategy and policy are designed to check if the desired C-SCRM outcomes have been achieved.

Business and Mission Impact Lastly, measures that are relevant to the company's strategic objectives.

While using this guideline might not be the right fit for every organisation, it is a good starting point for secure procurement.

4.3 Procurement guidelines for cybersecurity in hospitals

The report "Procurement guidelines for cybersecurity in hospitals" by ENISA is a collection of advice gathered from interviews with subject matter experts. The overall goal of the report is to provide staff that operates in technical positions in healthcare organisations with guidelines to on how to improve the acquisition process. While the report is specifically tailored towards hospitals, the overall procurement process as is described here is not. For our thesis we can adopt the advice from this report for general guidance on secure IT procurement [13, pp. 7–8].

The ENISA Procurement guidelines lay out a simple and concise lifecycle for the procurement process in hospitals: The Plan phase, the source phase and the manage phase [13, p. 11].

In the Plan phase business needs are analysed and necessary cyber security requirements are collected. In the Source phase, those requirements are then transformed into technical specifications, offers are being collected, evaluated and negotiated, and a solution is chosen. Lastly, in the manage phase, an owner is chosen that will be responsible for the continuous management of the product or service in terms of incidents, vulnerabilities, patching and performance [13, p. 12].

Next come a number of *"Good Practices for cybersecurity in Procurement"* [13, p. 28] and a small clarification. While the ENISA Procurement guidelines [13] lay out 30 different good practices for procurement, we will focus on what we deem to be the most important one's [13, pp. 29–45].

GP 2. Implement a vulnerability identification and management process Establish a process vulnerability identification and management. For each procured product or service, vulnerabilities should be found and monitored [13, p. 29].

GP 5. Establish testing policies Each product or service to be procured should run through a minimum set of security tests. Penetration tests should also be conducted once the product or service is in place [13, p. 31].

GP 6. Establish Business Continuity plans As part of the procurement process the failure of a system should be factored in so that incidents can be mitigated more easily [13, p. 32].

GP 11. Conduct a risk assessment as part of the procurement process For each product or service to be procured a risk assessment should take place so that risks are identified and later managed [13, p. 35]**.**

GP 13. Identify threats related to procurement products or services In the procurement process threats need to be identified and considered. This is a continuous process even after the procurement of a product or service has finished [13, p. 36].

GP 16. Establish eligibility criteria for suppliers For each supplier, criteria should be defined that test eligibility. Non-negotiable minimum security requirements should lead to suppliers being excluded if they cannot support a baseline of security [13, p. 38].

GP 21. Provide cybersecurity training on the organization's security practices to staff and external consultants The internal and external staff of the enterprise should receive adequate training on practicing secure procurement as well as the specific cyber security practices at the organisation [13, p. 40].

GP 22. Develop incident response plans Similar to Business Continuity plans, there should also be plans put in place in case of an incident regarding procured products or services [13, p. 41].

GP 26. Require patching for all components A crucial but often overlooked requirement for acquired products and services are software updates. The supplier should be compelled to share information about the patching process. As both scheduled and emergency patches are necessary, those should also be factored in as a time of unavailability of the product or service [13, p. 43].

GP 28. Perform asset inventory and configuration management All assets should be documented in a type of inventory management system. Any added products or services should also be added to the inventory management system. Furthermore, default configurations should be created and documented for each type of procured component [13, p. 44].

ENISA lays out excellent on the lifecycle and good practices in the procurement process. While the information is very specific to the healthcare sector, it is still a massive enrichment any enterprise looking for cyber security improvements.

4.4 ENISA cybersecurity market analysis framework

The ENISA cybersecurity market analysis framework is a 2021 publication that aims to provide guidelines on how to conduct cyber security market analysis in the European Union. The market analysis framework is structured into six modules that each focus on different aspects cyber security market analysis [14, p. 5].

Market Structure and Segmentation:

In this phase we scope out the market analysis. We mainly determine what elements from the cyber security value chain we consider, and which segments of the value stack are contributing to the value chain [14, pp. 13–14].

Demand-side research:

This module attempts to gather relevant market data from an end-user's point of view about cyber security products, services and processes. This also includes the value chain and the value stack that we have scoped out int the previous module. What we achieve from Demand-side research is information about demand volume and growth, market trends, cybersecurity maturity and common security requirements [14, pp. 15–17].

Supply-side research:

Supply-side research on the other hand is attempting to analyse the suppliers of cybersecurity products and services. The outcomes of the supply-side research should be that supplier types are selected, a supplier mapping is created and analysis reports on suppliers are drawn up [14, pp. 17–18].

Technology research:

The goal of technology research is to gauge the possible future impact of technological advancements on the cyber security market [14, p. 19].

Macro-Environmental Factors and Economic Market Characteristics:

In these modules, analysis frameworks like PEST are used to consider multiple perspectives to get an overview of current and possible future trends [14, p. 21].

Market analysis is a great way to gauge what cyber security related issues currently exist and what products and services are being provided to alleviate those issues. This in turn can in turn can help, if used correctly, provide context for the procurement department's processes.

4.5 Secure ICT procurement in electronic communications

This publication from 2014 by ENISA is a survey of providers and vendors on secure ICT procurement and a collection of recommendations that are based on this survey. While the publication itself focuses on other topics of secure procurement as well, this thesis will focus only on the results of the survey and the recommendations stemming from these results [15, p. iii].

The results of the survey are structured as an exemplary framework that focuses on 4 main areas: Risk Assessment, Security Requirements, Performance Monitoring and Change Management [15, p. 21].

Generally, regulators and standardisation bodies recommend conducting risk assessments before procuring a product or service. A proper risk assessment will help a procurement department in evaluating a supplier's security measures and whether those measures align with the procuring company's strategy and policies [15, pp. 21–22].

After risk management, high level security requirements should be put in place so that a preferred vendor can be selected. This ensures that vendors know whether they will be able to fulfil the desired security requirement before further negotiations take place. In the final contract those requirements will then be included in a more refined and detailed manner [15, pp. 22–23].

While trust is an important factor in any supplier relationship, agreements and contracts must be verified for compliance. Information will have to be provided to the procurer by the vendor, so that the requirements of the contract can be verified. Based on the verification, corrections can then be issued where needed [15, pp. 27–26].

As part of supplier relationship management, ENISA also discovers, through the survey, that a change in the supplier relationship also should be managed suitably. These changes can occur due to a variety of reasons and may also encompass changes to the security requirements as defined in the contract. A process should be defined to facilitate changes to the security requirements if necessary. A special kind of change to the supplier relationship is the termination of the contract. Processes for a secure termination also need to be agreed upon in the contract [15, p. 28].

Based on the results of the survey, ENISA gives out several detailed recommendations on practicing secure ICT procurement:

Develop a holistic risk management approach with internal stakeholders:

Relevant stakeholders should be involved at every stage of the procurement process. Furthermore, procurement security practices need to be implemented in the whole company, not just in the procurement department itself [15, p. 30].

Conduct risk assessments before procurement:

As determined through the survey, it is generally advised to undertake a risk assessment before the procurement process for a product or service starts. This will aid significantly in defining security policies and requirements that combat specific risks that the company faces [15, p. 30].

Develop security policies and requirements before procurement:

Based on a risk assessment, high level security policies and requirements should be defined before approaching or being approached by a potential vendor. This will help to focus the procurement efforts on suppliers that are capable of fulfilling the essential security requirements. This approach helps to allocate procurement resources much more efficiently [15, p. 31].

Develop security requirements for vendors:

Any security polices and requirements should be clear, concise, measurable and actionable. This helps to ensure that the supplier of the product or service can comply with those policies or measures. Ideally, changes to the security requirements will not be necessary since changes can introduce uncertainty and worse security practises [15, p. 31].

Manage risks throughout the lifecycle of procurement:

While it is tempting to only practice secure ICT procurement during the vendor vetting process, it is crucial for the success of procurement to establish security measures at all stages of a product or service lifecycle [15, p. 31].

Monitor the performance of suppliers:

Continuous monitoring is necessary to make sure that the supplier of a product or service is compliant with the agreed upon security requirements and policies. If deficiencies are found corrective actions or penalties can be administered.

4.6 ENISA Security Guide for ICT Procurement

The indented audience for this publication from 2014 are vendors of ICT products. It is a collection of practices, gathered through a survey, that aim to aid in the secure procurement of ICT for vendors. The main goal is to mitigate risks that arise from the supply chain [16, p. 1].

The security guide consists of a list of security requirements that address common security risks for vendors emanating from suppliers [16, pp. 3–20]:

- Information security policies
- Security requirements in contract
- Risk assessments
- Roles and Responsibilities are defined
- Vendor employees training
- Managing of risks from change in employment status of vendor's employees
- Physical security
- Access control to IT systems
- Integrity validation of IT systems
- Change management processes should be properly defined
- Contingency Plan for termination of relationship
- Process for asset management
- Incident management procedures
- Incident reporting
- Business continuity strategies
- Disaster recovery plans
- Monitoring policies
- Testing
- Compliance Monitoring

Using this set of guidelines can greatly improve the risk mitigation strategy and procurement process for suppliers regardless of whether the procurer is a vender or not. The presented practices can still be applied to all procurers.

4.7 Österreichisches Informationssicherheitshandbuch

This publication from 2022 is a collection of guidelines for information security practices adapted to the individual requirements of the environment. The version 4.3.2 was used for this evaluation. While the work is not specific to procurement, it contains a section on procurement practices that aim to aid in practicing secure procurement.

According to the Austrian information security handbook, a secure acquisition process could be structured into 10 different phases [17, p. 745]:

- Planning and initiation of the procurement
- Determination of a need
- Conduct market research
- Derive product requirements
- Decide on Make-or-Buy-decision
- Handle contractual aspects
- Delivery management and monitoring
- Testing and acceptance
- Conclude procurement process
- Evaluate the procurement process and product

The publication also proposes several baseline security standards for the procurement of products [17, pp. 746–747]. These are however directly taken from an ENISA guideline [18] so those will be covered in a section 4.8.

As with many other guidelines and frameworks, the Austrian information security handbook also recommends conducting risk analysis as part of the procurement process before any potential suppliers are contacted [17, p. 747].

Furthermore, the handbook lays out a numerous examples for security risks for typical types of products that are procured [17, pp. 747–748]. We will only cover the crucial risks:

Table 2 Security risks for different types of software

Type of Product	IT security risks
Commercial off-the-shelf	▪ Vendor lock-in ▪ Blackbox system ▪ Needless features could become security risks ▪ IT security added as an afterthought ▪ Complex integration ▪ Error prone deployments ▪ Complex change management
Government off-the-shelf	▪ Low customizability due to standardised approach ▪ High costs of customization ▪ Many stakeholders involved
Individual new development	▪ Missing know-how within ▪ Time intensive ▪ High degree of specialization necessary
Individual adaptations of an existing product	▪ Complex Customizations necessary ▪ Needless features could become security risks ▪ Poor integrations
Open-Source Product	▪ Vulnerabilities are known to the public ▪ Complex licensing ▪ Little to no technical support ▪ No guarantee of continuous development

With these measures the overall effectiveness of procurement practices can be greatly improved and the adaptation of secure procurement into the procurement process supported.

4.8 Indispensable baseline security requirements for the procurement of secure ICT products and services

This publication from 2016 is a set of baseline security requirements that help facilitate secure procurement of ICT products. The general recommendation is that if any of these security requirements are not or cannot be fulfilled by the supplier, then those products or services should not be considered a viable solution. The proposed requirements are not a replacement for certification standards but should be viewed more as a baseline [18, p. 1].

Security by design:

Each product or service should be designed and configured based on proven security practices. ENISA also sees a minimal set of functionalities as part of security by design [18, p. 5].

Least privilege:

Access should follow the least privilege principle. The suppliers should only have access when it is absolutely needed for administration. Managing the service or product should be handled by the procuring company themself [18, p. 5].

Strong authentication:

Strong authentication as well as authorisation mechanisms should be in place in any product or service. Furthermore service accounts should be separated from normal interactive login accounts [18, p. 6].

Asset Protection:

Data should be encrypted at rest as well as in transit. The encryption that is used must be state-of-the-art and contain no known vulnerabilities [18, p. 6].

Supply chain Security:

Just like a procurer is interested in ensuring good security practises at the vendor, it is also desirable to ensure that suppliers of the vendor also practise good security. Vendors should be required to practice ongoing integrity and authenticity checks [18, p. 7].

Document Transparency:

To verify the compliance of all security requirements and policies, vendors and suppliers must provide proper documentation about the product or service. The documentation also must be updated when changes occur [18, p. 7].

Quality Management:

The supplier should be able to show that quality management is practised in an adequate manner. This could be shown by following a certification standard like ISO 27001 [18, pp. 7–8].

Service Continuity:

The procurer must be able to expect continuous support throughout the lifecycle of the procurement [18, p. 8].

While these security requirements do not guarantee a fully secure and resilient product or service, it is a good start for a procurer to design their own individualised security requirements and policies.

4.9 Notional Supply Chain Risk Management Practices for Federal Information Systems

This publication is a collection of practices to facilitate the integration of risk management factors into the procurement of information and communications technologies (ICTs) for US federal departments and agencies. The core of the document are ten supply chain risk management practices than can be used for an ICT procurement strategy [19, pp. 2, 25].

Uniquely Identify Supply Chain Elements, Processes, and Actors:

It is imperative to provide context to the environment that the procurement processes take place in. Only with enough visibility into the supply chain can context be provided[19, p. 28].

Limit Access and Exposure within the Supply Chain:

According to the publication access to products should be limited withing the supply chain. Since a lot of personnel must access products to perform their roles, access control and monitoring should be practiced [19, p. 31].

Establish and Maintain the Provenance of Elements, Processes, Tools, and Data:

Proper documentation needs to exist for each system elements. This includes, but is not limited to, the source, the change history and who had the possibility of changing a system [19, p. 34].

Share Information within Strict Limits:

The publication acknowledges that information sharing needs to take place for a secure procurement process to happen. To prevent information from falling into the hands of threat actors, shared information should be protected. One way this could be achieved, is by all parties aggreging to ensure that information is protected appropriately [19, pp. 38–39].

Perform Supply Chain Risk Management Awareness and Training:

Any supply chain risk mitigation strategy needs to be supported by rigorous training. Without proper awareness and training, policies stemming from the mitigation strategy will not be followed effectively and the strategy may underperform as a result [19, pp. 45–46].

Use Defensive Design for Systems, Elements, and Processes:

The general goal of using defensive design techniques is to inhibit the impact of attacks to contingent systems, elements or processes. Using defensive design concepts also helps deal with uncertainty and maintains a level of flexibility to adapt to changes to the environment [19, p. 48].

Perform Continuous Integrator Review:

The publication also points out an important distinction: The entity that is supplying the element or system can be different from the entity that is integrating the element or system into the environment of the procurer. This means that not only suppliers but also integrators need to be reviewed and their compliance to requirements needs to be validated [19, p. 58].

Strengthen Delivery Mechanisms:

Delivery can be classified into two types: physical (like hardware) and logical (like patches). Both delivery types can be compromised along the supply chain or even the lifecycle of a system or element. Therefore, steps should be taken to ensure the security of delivery mechanisms [19, pp. 61–62].

Assure Sustainment Activities and Processes:

The procurement process is not completed after a system or element has been acquired. The process continues until the system or element has been disposed of. Within those two points in time, supply chain risks occur through activities like maintenance, patching or upgrades. Processes should exist that help ensure the confidentiality, integrity and availability during those activities [19, p. 65].

Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle:

After a product's use has expired, sensitive information and data still need to be properly disposed of. The rules for disposal of procured products should be created by the procurer. Often, this activity is overlooked and disposal is not done in a manner that is aware of supply chain threats and risks [19, pp. 70–71].

The practices are intended to be used in conjunction with other NIST risk management methods. Still using these supply chain practices on their own can greatly aid in developing an effective procurement lifecycle.

4.10 Cloud Computing Kompass

This publication is a set of guidelines from A-SIT Plus GmbH for Austrian cloud service customers. It covers cloud basics, strategy planning, requirements criteria and further information.

For the Cloud Computing Kompass, the first step of strategic planning is to evaluate the level of criticality for outsourced data and data applications. The level of criticality depends on the possible damages that can occur from a breach of confidentiality, integrity, or availability in the business processes of the organisation [20, p. 16].

After the level of criticality has been established, the next step is the requirements analysis. Here, legal obligations and operational conditions are identified and analysed [20, p. 20].

Next, a risk analysis is conducted that assesses all relevant threats and vulnerability to the assets of the organisation. Assets include, but are not limited to: data, information systems or business processes [20, p. 31].

Lastly, the Cloud Computing Kompass specifically defines a data protection impact assessment as part of the strategic planning. Here, risks are to be identified and analysed as they relate to the impacted parties [20, p. 34].

The document also presents a considerable amount of requirement criteria that can be used for contractual agreements between procurers and cloud service providers [20, p. 41].

Generally, outsourcing data and applications to the cloud involves special challenges that come with that decision. Those challenges can be of technical, organisational, or even legal nature. The Cloud Computing Kompass is a useful

procurement tool than can help greatly in selecting suppliers of cloud services from the point of security.

4.11 ISO/IEC 27036

The standard consists of 4 documents that offer guidance on different parts in supplier relationship management. While part one and two offer guidance on supplier relationship management in general, part three and four offer guidelines for ICT supply chain security and security of cloud services respectively with specific security controls [21, p. 10].

Part 3 is introducing supply chain security concepts for the procurement of information communication technology products. The document also presents supply chain security practices that are crucial for any information communication technology procurement process [22, p. 6]:

- Chain of custody
- Least privilege access
- Separation of duties
- Integrity protection
- Managing compliance
- Vulnerability Assessment
- Vulnerability Management
- Clear Roles & Responsibilities
- Anonymous acquisition

Part 4 is making a distinction between different cloud deployment models. Depending on the type of service provided, IaaS, PaaS or SaaS, a different set of controls is proposed. Generally, the lower level the service is the more controls are deemed essential. The controls presented are intended to be used by cloud service providers offering services, not for procurers. Therefore, those controls will not be discussed in further detail [23, pp. 12–14].

4.12 The Software Supply Chain Integrity Framework

This publication from 2009 by SAFECode is defining a small framework to address common risks stemming from the supply chain. The focus of this publication is not

to define a procurement framework for an individual organisation but to create a mode of operation that is used amongst an entire ecosystem.

SAFECode has determined that a usual software development process involves combining components from many different suppliers. These suppliers have also sourced components from many different suppliers. This creates a lot of complexity that must be managed. Two ways this can be achieved is to either use a Software Bill of Materials (SBOM) or to use supply management processes to implement controls. These controls would then be applied between each link from one supplier to the next until the Customer is reached. This would allow for each transition to be accounted for [24, pp. 6–7].

According to the publication the controls that should be applied when a component is within each supplier's control are as follows [24, p. 10]:

- "Chain of Custody"
- "Least Privilege Access"
- "Separation of Duties"
- "Tamper Resistance and Evidence"
- "Persistent Protection"
- "Compliance Management"
- "Code Testing and Verification"

Having these shared and complementary efforts in place would greatly improve the overall maturity of the entire market. This however would require the cooperation of many different software suppliers, integrators, and procurers.

4.13 Procurement guide for secure AI components

The IEEE paper published in 2022 is mainly offering guidance for the requirements that stem from the proposed AI Act [9] by the European Commission. Furthermore, evaluation criteria are given that can be used during the procurement process to fulfil the requirements of the AI Act.

Categorization of the implemented AI methods:

The actual purpose of this criteria is not to categorize the used AI methods but to quickly eliminate those suppliers that lack the required competency to offer an adequate AI solution. Furthermore it helps determine the level of competency at which the software itself operates [25, p. 3].

Deployment and maintenance:

Here it is important to assess not only the deployment but also how the continued maintenance is handled [25, p. 3].

Execution context:

To be able to conduct proper risk management and threat analysis, the context in which the AI system will be integrated into must be evaluated [25, p. 4].

Source Code:

It might be beneficial to request the source code of the AI solution. This enables to procurer to by themselves evaluate the quality of the solution and make adjustments to their environment to mitigate vulnerabilities [25, pp. 4–5].

Interfaces:

As the AI solution will most likely be interacting with other systems within the procuring organisation's environment, it is vital to manage the interfaces of such a solution properly [25, p. 4].

Integrity protection, Audit & Control:

A common attack for AI solutions is to poison the input data. Audit & Control mechanisms can be used to assess the integrity protection that aims to defend against such types of attacks [25, p. 4].

Privacy:

Depending on the sensitivity of the data that is handled by the AI solution, privacy protection can be a key criterion [25, pp. 4–5].

Training data:

While the integrity of data is already covered by the "Integrity protection, Audit & Control" criterion, it is also important to specifically take a look at the trustworthiness of training data to be used [25, p. 5].

The different possible applications for Artificial Intelligence are still vastly growing. Furthermore, the number of suppliers each organization is dependant upon is also vastly growing. Therefore, proposed solutions, like this paper, for issues in specific areas of procurement will be necessary so that organizations can conduct secure IT procurement as a whole.

4.14 Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf Teil 1 Version 2.0

The publication by the BSI is a collection of practices for critical internal telecommunication systems. As the name of the publication already suggests, the intended use is to take the defined criteria and adapt them to the organisation's individual needs. The guidance is very specific to telecommunication systems and even more specific to the exact type of telecommunication system that is being procured. The publication is most useful when the exact type of solution that is needed is already known [26].

While the guideline is tailored towards the procurement of telecommunication systems, some general practices about procurement can still be extracted.

Select telecommunication solutions under consideration of security aspects:

Many products and services can be secured with good planning and technical measures. Sometimes that is not possible. Those cases need to be considered separately. This may be an exclusion criterion for a product or service [26, p. 311].

Incorporating the server of a telecommunication solution into the patch management of the organisation:

Managing software patches is an inevitability in any asset that contains software. If a solution is interfacing other solutions, it is important to reconcile the advantages of security and feature updates with the possibility of affecting the availability of the entire system [26, p. 315].

Secure retirement of components of the telecommunication system:

During the lifetime of a component data is often gathered and stored on the devices. After a component has fulfilled its purpose, all relevant data needs to be irreversibly deleted [26, p. 318].

Proof of trustworthiness of the supplier:

Using certifications like ISO 27001, trustworthiness can be demonstrated by a supplier [26, p. 318].

Training of Administrators for telecommunication solutions:

Telecommunication systems cannot be considered individually. Changes within one component can have significant impact on other components in the system. It

is therefore necessary to train administrators on the interaction between individual components and the entire system [26, p. 322].

Generally, the publication sees a trend that more and more telecommunication applications more towards the public cloud where the implementation of controls by procurers is much more difficult and needs to be addresses in a different manner [26, p. 344].

4.15 Study on the need of Cybersecurity requirement for ICT products

This report is the summary of a study that was conducted for the European Commission in 2021. The goal of the study was to create guidance for the European Commission on the possible policy options and their effects on the cybersecurity market of the European Union [27, p. 22].

To support the report's main goal to make recommendations for European lawmakers, essential requirements are introduced that aim to ensure product security [27, pp. 136–137]:

- Security by Design
- Reduce attack surface
- Robust identity and access management
- Data protection
- Awareness training
- Ensure resilience
- Monitoring
- Continuous improvement

Each essential requirement is aided by security requirements that aim to implement the essential requirements [27, p. 141]. The security requirements are very comprehensive and partly consist of very technical measures. Therefore, those will not be covered in this thesis and can be examined for designing the requirements for a procurement when needed.

The publication covers a wide area of cybersecurity policymaking that is not directly related to a company's procurement process. It is however possible to draw must-have security requirements for procured products and services.

4.16 NPSA Protected Procurement

This publication is a booklet on practicing secure procurement by the National Protective Security Authority (NPSA) in the United Kingdom. The goal is to offer guidance on how to incorporate security practices into the existing procurement processes [19, p. 5].

Oversight:

For all procurement activities to have cyber security in mind, governance needs to be implemented that establishes secure procurement processes while incorporating the procurement team, senior management and operational teams. Furthermore, policies need to be put in place that aid selecting suppliers. Lastly, activities like awareness training should be conducted to form a security culture at the organisation [28, p. 9].

Outsourcing decision:

When the decision to outsource is taking place, several activities should be taking place [28, pp. 11–21]:

- Threat assessments
- Risk assessments
- Determining the necessary security level

Supplier selection:

Self-assessment questionnaires for suppliers can help quickly weeding out suppliers that do not fulfil the basic security requirements. Of course, those requirements still need to be contractually clarified and their compliance audited [28, p. 23].

Contracts:

Within the contract with the supplier, certain topics should be contained to avoid disputes in the future [28, p. 25]:

- Security Requirements
- Incident Notification
- Independent Reviews
- Termination

Supplier Performance:

Having contractual agreements also requires monitoring on whether or not those contractual agreements are adhered to. One of the most effective ways to achieve

this is through audits and stress testing. Incident Management should also be practised effectively to increase resilience and reduce the impact of an incident [28, pp. 27–28].

Termination:

As mentioned before, termination clauses should exist any contract with suppliers of products or services. These clauses can either be triggered by the natural ending of a contract or by special cases like a breach of contract [28, p. 31].

In their booklet, the NPSA also provides further guidance on the topic of secure procurement in the form of brochures, booklists, checklists and questionnaires.

4.17 ENISA Procure Secure

This document is a set of guidelines by ENSIA for secure procurement concerning cloud services. Specifically, the focus lies on monitoring service level agreements and contracts. While the document's main concerns are cloud services, plenty of guidance on performance monitoring in procurement can be drawn [29, p. 5].

The publication is suggesting a set of parameters that can be used to monitor the security measures effectiveness of the cloud service provider. Depending on the type of cloud service to be procured SaaS, PaaS or IaaS, different parameters need to be prioritised [29, p. 11].

Service availability:

Availability requirements must be defined in the service level agreement with the cloud service provider. This ensures that the cloud service provider and procurer have the same understanding of what availability means for the service and how availability compliance will be verified. As part of the design process for the availability requirements, a risk profile should be created to define the criticality of the service. The risk profile could also include other requirements like performance requirements [29, pp. 14–15].

Incident response:

When an event takes place that is not within the normal operation as defined in the service level agreement, incident response should take place to mitigate the incident. Incident response can take many different forms and has plenty of parameters that have to be considered [29, p. 20].

Service Elasticity and load tolerance:

To ensure the desired availability of the procurer, flexibility in terms of computing resources should be another major factor. A commitment of the cloud service provider to be able to handle future loads should also be given where possible. This helps to ensure that a service remains available, even when utilization increases [29, p. 24].

Data lifecycle management:

These parameters should assess how data is managed by the cloud service provider [29, p. 31].

Technical compliance and vulnerability management:

While basic requirements like adhering to a security policy and successfully managing vulnerabilities should of course be followed, it is also instrumental that customers are given the tools to apply customer-side workarounds to temporarily close vulnerabilities until patches are rolled out [29, p. 34].

Change-management:

Any significant changes to the service level agreement should be influenced by several parameters [29, p. 40]:

- Change management process testing
- Change notice time
- Change triggers
- Time to implement requests by the customer

Data Isolation:

As cloud service providers usually handle more than one customer, resources are often shared between customers. Still, customer data needs to be isolated from each other to establish availability, confidentiality and integrity. Depending on the type of services provided, the technical means to achieve this are vastly different [29, p. 42].

Log management and forensics:

Logs about the customers service should exist and be given to the customer. While the document does not define what is being collected in those logs, it does suggest for an agreement to be in place between the cloud service provider and the customer. And, part of that agreement should be a detailed account of what logs are created and provided to the customer [29, p. 45].

After defining all suggested parameters, the publication also includes a checklist with which all those parameters can be covered. The checklist is a series of questions to be answered by the cloud service provider. Based on that a procurement decision from the point of security can be made. This does not replace the need for other, general requirements.

4.18 OWASP Software Component Verification Standard

This publication is a 2020 standard that aims to aid in risk identification and risk management for software development. The standard is using six different control families to cover a broad area of risk management. Companies can then use those controls during their procurement process as a parameter for selecting suppliers [30, p. 4].

Inventory Requirements:

Here, the overall goal is to obtain and keep an accurate inventory of all software components used in the development of the software [30, p. 8].

Software Bill of Materials Requirements:

A SBOM should be present and automated. What kind of format is used and whether or not multiple formats are used in conjunction depend on the specific use case [30, pp. 8–9].

Build Environment Requirements:

Build pipelines offer a large attack surface with their many different components that work together to build software. Build pipelines for software should be hardened against attackers [30, p. 10].

Package Management Requirements:

While the main purpose for package managers is to distribute software components and handle the different versions of those software components, it can also have vast security benefits. Those package managers need to be secured against attackers, to profit from those security benefits [30, p. 11].

Component Analysis Requirements:

Risk analysis practices should be conducted for all software components. Risks may also be inherited from 3rd party software and special care should be taken when the procured software is open source [30, pp. 12–13].

Pedigree and Provenance Requirements:

To notice when a supply chain has been compromised, the point of origin for each component has to be known. This way, mitigation can happen before an adverse effect is noticeable [30, p. 14].

The standard also introduces three different verification levels. Each verification level contains a different set of controls from the six control families. Higher levels are for software components that possess higher security requirements [30, p. 4].

If open-source software components are in use an open-source policy is needed, since open-source code poses unique risks that need to be addressed specifically.

Using these measures as a flexible checklist for procurement, supply chain security can improve drastically. The measures are also not intended to be implemented all at once. A procurer can incrementally increase the number of controls in effect until the desired verification level has been archived.

4.19 OWASP Application Security Verification Standard

This publication is a widespread 2021 OWASP standard for application security. The standard consists of security requirements that cover a wide area of application security.

While the standard has other uses as well, one of the use cases is to utilize the standard as a checklist for secure procurement. Suppliers can be asked to fulfil a certain ASVS level, depending on the criticality of the environment or the system [31, p. 16].

A crucial factor to consider when choosing the ASVS as a tool for secure procurement is that the standard is not certifiable by OWASP. 3rd parties, however, offer the service to verify the compliance of the standard to offer credibility to the answers to the checklist.

4.20 ACSC Information Security Manual

This work is a framework for practicing information security created by the Australian Cyber Security Centre in 2023. It is intended as a set of guidelines that can be used by businesses in conjunction with their own risk management frameworks. While the information security manual is not a document specific to

the secure procurement of IT systems, it is covering a wide range of security relevant topics [32, p. 1].

The manual proposes several typical practices for procurement [32, pp. 17–22]:

- Supply chain risk management
- Supplier relationship management
- Assessments for suppliers of products and services
- Contractual security requirements
- Managing access to internal systems and data by a service provider

The manual is using the risk management based approach from NIST SP 800-37 Rev.2 and is therefore giving similar guidance as the special publications from NIST [32, p. 2].

4.21 Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities

This publication is a set of communication guidelines during procurement of systems for the federal government of the United States. The report was created in May 2019 for the Department of Energy as an addition to the Task Order Request for Proposal that normally communicates terms and conditions [33, p. 4]. While the publication is not intended to be used as secure procurement guidelines, criteria can still be extracted from it.

According to the guidelines several key factors should be considered when a procurement contract is negotiated [33, p. 9]:

- List of security features of procured products should be provided
- Guidance on secure configurations
- Incident reporting and resolution
- Restriction of network traffic between different security zones
- Removal of unnecessary software components
- Least privilege principle
- Default settings should be customised for each procurer

The publication also suggests a procurement lifecycle consisting of designing, developing, procuring, storing, delivering, implementing, maintaining and retiring

phases. All of these phases together can lead to a stronger and more mature system in terms of cybersecurity [33, pp. 9–10].

4.22 Beschaffung unter Berücksichtigung der IT Sicherheit

This book from 2017 is outlining a framework for practicing secure IT procurement. The framework is intended to be applied for the procurement of products that contain any kind of software [34, p. 7].

The book outlines several critical practices for secure procurement of IT systems [34, pp. 22–30]:

- Risk analysis
- Assessing level of criticality
- Creating security requirements
- Product certifications
- SLAs
- Incident management
- Business continuity plans
- Security tests
- Contract change management

These practices can lead to a significant drop in risk stemming from the supply chain. Once procurers start implementing and requiring these practices, suppliers will soon follow to stay competitive [34, p. 54].

4.23 STAR Level 1: Security Questionnaire

This publication is a set of questions targeted towards providers of cloud services. The questions aim is to determine what controls exist for the offered cloud services. Based on the answers to these questions, procurers can then make an informed decision on which supplier to choose [35].

4.24 ISO 15408

This ISO standard is a set of requirements for security functionality or IT products and measures to ensure trust. It is intended to increase the comparability of the

results of security evaluation. Therefore, it is useful for the secure procurement of IT systems. It is commonly referred to as “Common Criteria” [36, p. 7].

Evaluation Assurance Level (EAL) is a scale for evaluating the degree of trust versus costs for an IT system. The seven levels differ in strictness, scope, depth and the addition of further security requirements. A higher level indicates a higher level of trust [36, pp. 25–26].

EAL1 – functionally audited:

This level is best used when some level of trust is necessary for the proper operation, but security risks are not seen as serious. There are little to no security requirements at this trust level [36, p. 27].

EAL2 – structurally audited:

EAL2 incorporates the developer into the review process. The developer provides design information without using too much time or too many resources of the developer [36, p. 28].

EAL3 – methodically audited and reviewed:

This level demands for security engineering to play an important role during the design phase without adapting general development practices. This aims to create a moderate amount of security without requiring re-engineering [36, p. 29].

EAL4 – methodically developed, audited and reviewed:

EAL4 requires an extensive description of the design and improved development mechanisms and practices that demonstrate trust [36, p. 31].

EAL5 – semiformally developed and audited:

EAL5 uses strict development practices that are supported by the moderate application of engineering techniques. It requires the semiformal description of the design whose architecture is structured [36, p. 32].

EAL6 – semiformally verified design and audited:

This level is intended for creating high trust for very risky situation where the impact justifies the extra costs. EAL6 requires an extensive analysis, structured representation of the implementation and extensive independent vulnerability analysis [36, p. 34].

EAL7 – formally verified design and audited:

EAL7 is best used for very high risk or high impact situations. It requires the usage of a formal representation, formal correspondence and extensive review [36, p. 35].

Using these levels can provide a standardised way for procurers to evaluate IT systems against each other. The cost and the trust into the evaluation can be adapted depending on the budget and risk appetite of the procurer.

5 Criteria

Through the literature evaluation 69 different criteria for secure procurement were extracted from the reviewed documents. Most of these criteria occur in more than one document. Appendix A documents what documents lead to which criteria.

The criteria can be broadly sorted into six categories:

- Providing context
- Planning
- Security requirements for products and services
- Security requirements for suppliers
- Supplier relationship
- Ongoing managerial tasks

5.1 Providing Context

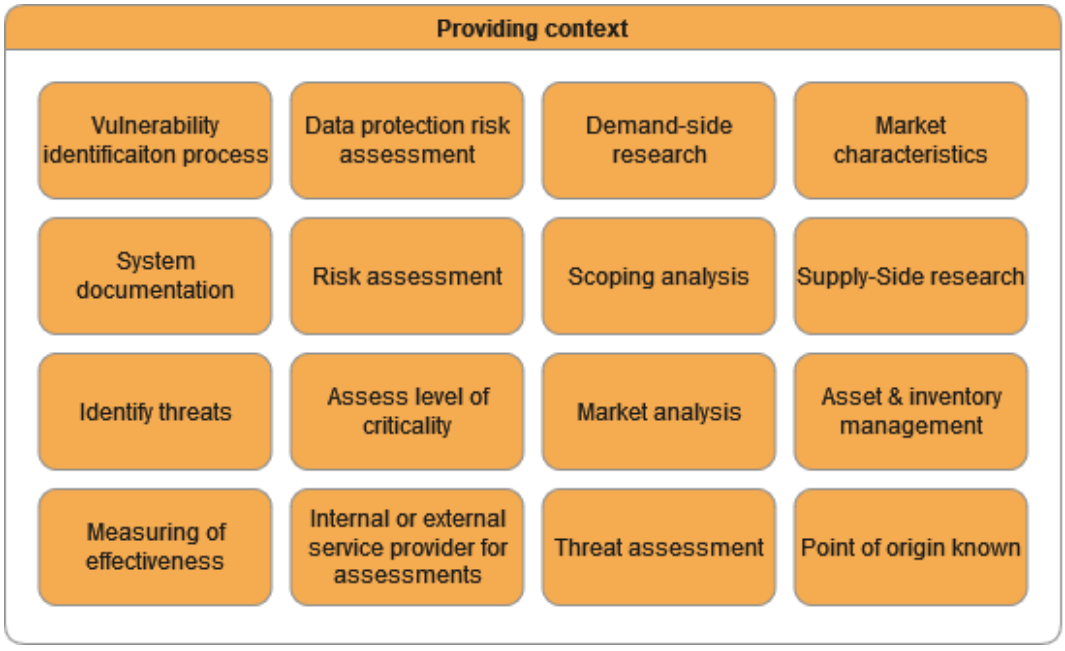


Figure 2 *Criteria in the "Providing context" category*

Activities that fall in the providing context category create a basis on which secure procurement processes can build upon. Without efficient assessments and analysis as displayed in Figure 2, essential data will be missing.

5.2 Planning

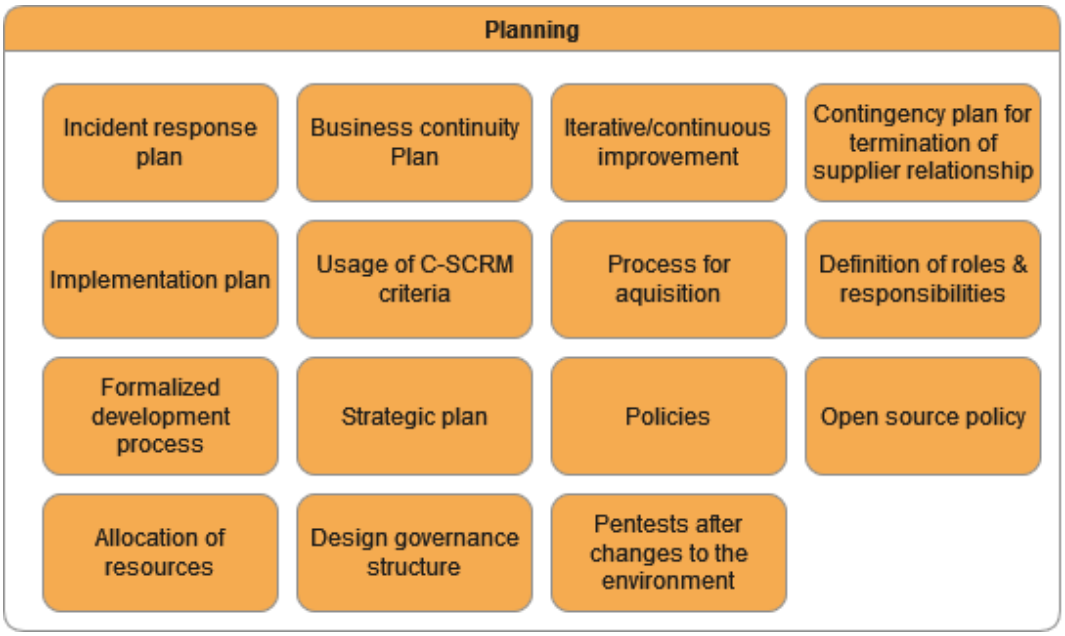


Figure 3 *Criteria in the "Planning" category*

Before implementation can happen, planning must take place with the help of criteria as described in Figure 3. Planning can take many different forms. Some of the forms are plans themselves but also activities like formalizing roles and processes can be forms of planning as well.

5.3 Security requirements for products and services

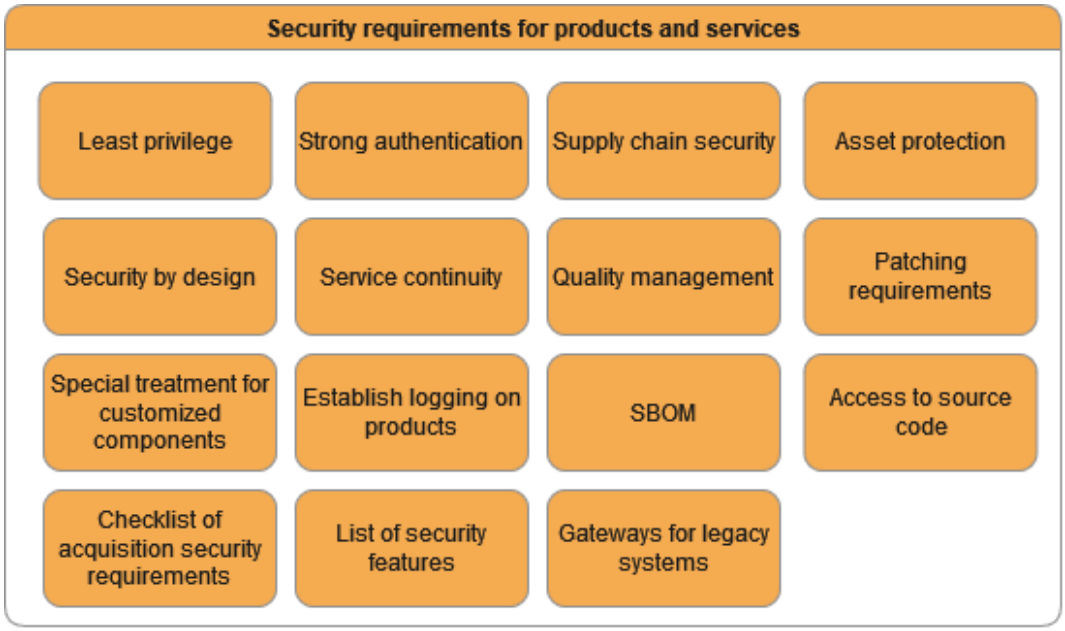


Figure 4 *Criteria in the "Security requirements for products and services" category*

To aid a procurer in selecting products or services, checklists with criteria can be used for the procurement process. What items the checklists consist of strongly depends on the type of product or service procured. Figure 4 gives and overview of some of the security requirements that could be relevant for an acquisition.

5.4 Security requirements for suppliers

Figure 5 *Criteria in the "Security requirements for suppliers" category*

Similar to the security requirements for products and services, checklists can also be used for defining security requirements that suppliers have to fulfill to be eligible as defined in Figure 5.

5.5 Supplier relationship

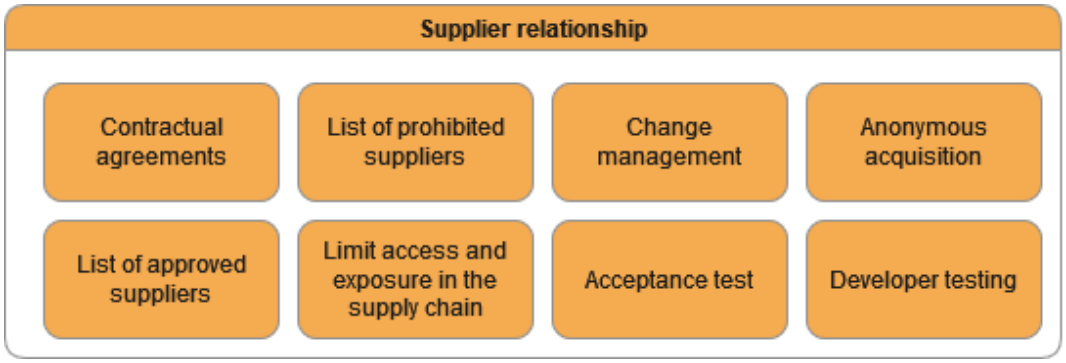


Figure 6 *Criteria in the "Supplier relationship" category*

Another big part of secure procurement is supplier relationship management. Like any other asset, relationships with suppliers need to be actively managed. Active management criteria can be found in Figure 6.

5.6 Ongoing managerial tasks

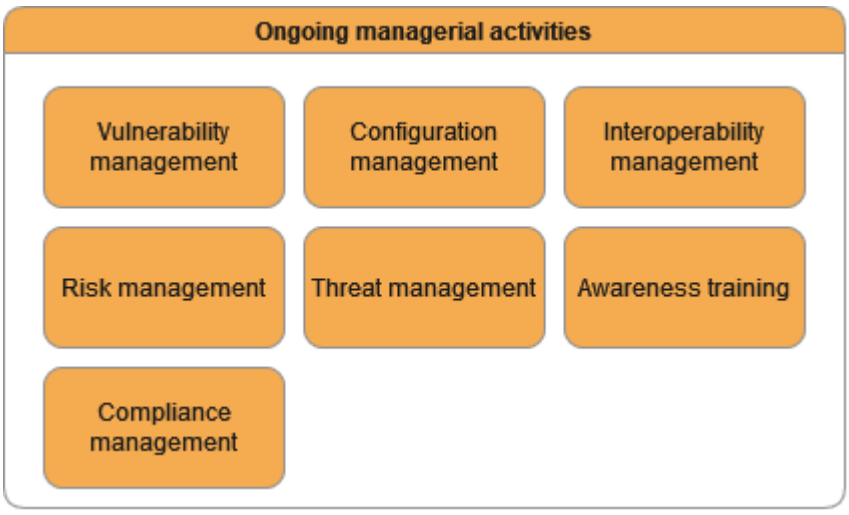


Figure 7 *Criteria in the "Ongoing managerial tasks" category*

Secure procurement is not completed after the procured service or product has been acquired and installed. Many managerial processes, as seen in Figure 7, should still be continued at least until the product or service has been retired.

6 Empirical Evaluation

In this section, the interviews that took place with SEC consult and PWC will be used to evaluate the created secure procurement criteria from section 5. One additional interview was conducted but consent was not given for their use in the thesis. Therefore, evaluation is only possible using two interviews.

Several Criteria were reaffirmed in the interviews:

- Acceptance tests
- Awareness trainings
- Certification requirements
- Checklists with security requirements
- Compliance management
- Contractual agreements
- Incident response plans
- Level of criticality
- Maintenance
- Patching requirements
- Special treatment for customised components
- Supplier Relationship management
- Threat assessment
- Vulnerability management

The interviews brough two additional essential criteria for secure IT procurement to light that have not been considered previously:

- Business impact analysis
- Prioritization of resources

The interviews also show that it may not be necessary to include 69 different secure procurement criteria in our proposed solution. My interview partners clearly demonstrated that the establishment of a basic secure procurement process with prioritization already puts the business ahead of most competitors. Including this many criteria might only lead to bloating of the secure procurement process.

7 Conclusion

As the prevalence of supply chain attack rises, secure procurement will become more and more important. Not only is there pressure from the economic side through threats but also increasingly from regulatory bodies. At the moment in the European Union, laws are being drafted that aim to increase the accountability of European businesses operating in the European market.

In this thesis several possible legal obligations for Austrian companies were analysed and evaluated. Furthermore, 69 different secure procurement criteria were created that are ready to be used by Austrian companies for their own procurement processes.

Due to the time constraints given by a master thesis secure procurement could not be considered in its entirety. While the criteria themselves are already useful for businesses, it would greatly expand their usefulness if those criteria were prioritised according to their potential beneficial impact to the procurement process.

Furthermore, the empirical evaluation section has shown that insights from secure procurement experts have not been sufficiently considered. There is still a large amount of practical data that those experts possess, that cannot be retrieved from standards and guidelines alone.

References

[1] 'NVD - CVE-2023-34362'. https://nvd.nist.gov/vuln/detail/CVE-2023-34362 (accessed Jun. 07, 2023).

[2] 'MOVEit hack: BBC, BA and Boots among cyber attack victims', *BBC News*, Jun. 05, 2023. Accessed: Jun. 07, 2023. [Online]. Available: https://www.bbc.com/news/technology-65814104

[3] M. J. Page *et al.*, 'The PRISMA 2020 statement: an updated guideline for reporting systematic reviews', *Syst Rev*, vol. 10, no. 1, p. 89, Dec. 2021, doi: 10.1186/s13643-021-01626-4.

[4] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. 2016. Accessed: Mar. 30, 2023. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng

[5] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)*, vol. 194. 2016. Accessed: Mar. 16, 2023. [Online]. Available: http://data.europa.eu/eli/dir/2016/1148/oj/eng

[6] *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) (Text with EEA relevance)*, vol. 333. 2022. Accessed: Mar. 16, 2023. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/eng

[7] NERC, *CIP-013-1 – Cyber Security - Supply Chain Risk Management NERC*. 2018. Accessed: Mar. 30, 2023. [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf

[8] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*. 2022. Accessed: Mar. 17, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

[9] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. 2021. Accessed: Mar. 25, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[10] Deutschland, Ed., *IT-Grundschutz-Kompendium*. in Unternehmen und Wirtschaft. Köln: Bundesanzeiger-Verl, 2023. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[11] Joint Task Force Transformation Initiative, ‘Managing information security risk :: organization, mission, and information system view’, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-39, 2011. doi: 10.6028/NIST.SP.800-39.
[12] J. M. Boyens, ‘Cybersecurity Supply Chain Risk Management for Systems and Organizations’, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-161r1, 2022. doi: 10.6028/NIST.SP.800-161r1.
[13] A. Drougkas, D. Liveri, A. Zisi, and P. Kyranoudi, *Procurement guidelines for cybersecurity in hospitals: good practices for the security of healthcare services*. Heraklion: ENISA, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services
[14] European Union Agency for Cybersecurity., *ENISA cybersecurity market analysis framework (ECSMAF).* LU: Publications Office, 2022. Accessed: Mar. 06, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/55221
[15] M. Dekker and C. Karsberg, *Secure ICT procurement in electronic communications analysis and recommendations for procuring ICT securely in the electronic communications sector*. Heraklion: ENISA, 2014.
[16] European Network and Information Security Agency ., *Security guide for ICT procurement: ICT procurement security guide for electronic communications service providers.* LU: Publications Office, 2014. Accessed: Mar. 06, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/994989
[17] A-SIT Zentrum für sichere Informationstechnologie, *Österreichisches Informationssicherheitshandbuch*. 2023. Accessed: Jun. 07, 2023. [Online]. Available: https://www.sicherheitshandbuch.gv.at/
[18] European Union Agency for Cybersecurity., *Indispensable baseline security requirements for the procurement of secure ICT products and services*. Publications Office, 2017. Accessed: Jun. 07, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services/@@download/fullReport
[19] J. Boyens, C. Paulsen, N. Bartol, S. A. Shankles, and R. Moorthy, ‘Notional Supply Chain Risk Management Practices for Federal Information Systems (NIST)’, National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 7622, Oct. 2012. doi: 10.6028/NIST.IR.7622.
[20] A-SIT Zentrum für sichere Informationstechnologie, ‘Cloud computing kompass’, 2018. Accessed: Jun. 07, 2023. [Online]. Available: https://www.onlinesicherheit.gv.at/dam/jcr:da65575d-d91a-4795-983b-c5e5a753bd80/Cloud-Computing-Kompass.pdf
[21] ‘ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships — Part 1: Overview and concepts’. 2021. [Online]. Available: https://shop.austrian-standards.at/action/de/public/details/707263/ISO_IEC_27036-1_2021_2021_09_09
[22] ‘ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security’. 2013. [Online]. Available: https://shop.austrian-standards.at/action/de/public/details/511260/ISO_IEC_27036-3_2013_2013_11_08
[23] ‘ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security

of cloud services'. 2016. [Online]. Available: https://shop.austrian-standards.at/action/de/public/details/584053/ISO_IEC_27036-4_2016_2016_09_28
[24] Stacy Simpson, Ed., 'Software Assurance Forum for Excellence in Code (SAFECode), The Software Supply Chain Integrity Framework, Defining Risks and Responsibilities for Securing Software in the Global Supply Chain', 2009. Accessed: Jun. 07, 2023. [Online]. Available: http://safecode.org/publication/SAFECode_Supply_Chain0709.pdf
[25] P. Kieseberg, C. Buttinger, L. Kaltenbrunner, M. Temper, and S. Tjoa, 'Security considerations for the procurement and acquisition of Artificial Intelligence (AI) systems', in *2022 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Jul. 2022, pp. 1–7. doi: 10.1109/FUZZ-IEEE55066.2022.9882675.
[26] Deutschland, *TLSTK II Teil 1: Darstellung und Bewertung der Sicherheitsmechanismen*. 2014. Accessed: Jun. 07, 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/TKAnlagen/TLSTK_II-Teil_1%E2%80%93Basiswissen.pdf?__blob=publicationFile&v=1
[27] European Commission. Directorate General for Communications Networks, Content and Technology., Wawestone, CEPS, CARSA, and ICF, *Study on the need of Cybersecurity requirements for ICT products: no. 2020 0715 : final study report.* LU: Publications Office, 2021. Accessed: Mar. 17, 2023. [Online]. Available: https://data.europa.eu/doi/10.2759/025330
[28] NPSA, 'Supply Chain Security for Practitioners'. https://www.npsa.gov.uk/protected-procurement-practitioners (accessed Mar. 06, 2023).
[29] European Union Agency for Cybersecurity., 'Procure Secure - A guide to monitoring of security service levels in cloud contracts', 2012. Accessed: Jun. 07, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/@@download/fullReport
[30] OWASP, 'OWASP Software Component Verification Standard Version 1.0', 2020. Accessed: Jun. 07, 2023. [Online]. Available: https://owasp.org/www-project-software-component-verification-standard/
[31] OWASP, 'OWASP Application Security Verification Standard 4.0.3', 2021. Accessed: Jun. 07, 2023. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/
[32] Australian Cyber Security Center, *ACSC Information Security Manual*. 2023. Accessed: Jun. 07, 2023. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2023-03/Information%20Security%20Manual%20-%20%28March%202023%29.pdf
[33] Michael Mylrea, JA Rotondo, and Sri Nikhil Gupta Gourisetti, *Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities May 2019*. 2019. Accessed: Jun. 07, 2023. [Online]. Available: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-28661.pdf
[34] E. Piller, *Beschaffung unter Berücksichtigung der IT-Sicherheit*. in essentials. Wiesbaden: Springer Fachmedien, 2017. doi: 10.1007/978-3-658-18599-2.
[35] Cloud Security Alliance, 'STAR Level 1: Security Questionnaire (CAIQ v4)'. 2021. Accessed: Jun. 07, 2023. [Online]. Available:

https://cloudsecurityalliance.org/artifacts/star-level-1-security-questionnaire-caiq-v4/
[36] ‘ÖVE/ÖNORM EN ISO/IEC 15408-3:2021 05 15 - Lesesaal - Austrian Standards’. 2021. [Online]. Available: https://shop.austrian-standards.at/action/de/public/details/697695/OEVE_OENORM_EN_ISO_IEC_15408-3_2021_05_15

List of Figures

List of Tables

Appendix

A. Criteria Origin Tables

Table 3 Providing context origin table

	NIST SP 800-161r1	Procurement guidelines for security in hospitals	Cybersecurity marketing analysis framework	Secure ICT Procurement	Informations-sicherheitshandbuch	Cloud Computing Kompass	Procurement guide for secure AI components	Study on Cybersecurity requirements for ICT	NPSA Protected Procurement	ENISA Procure Secure	OWASP SCVS	ACSC Information Security Manual	ENISA Security Guide for ICT Procurement	OWASP	Beschaffung u. Berück. der IT Sicherheit	ISO/IEC 27036
Assess level of criticality						x			x						x	
Asset & inventory management		x											x			

Data protection risk assessment		x		x			x	x				x				
Demand-side research			x													
Identify threats		x			x											
Internal or external service provider for assessments	x													x	x	
Market analysis			x		x											
Market characteristics			x													
Measure effectiveness	x			x	x			x	x	x			x			
Point of origin known											x					

Risk assessment		x		x	x	x	x		x		x	x	x			
Scoping analysis			x		x											
Supply-side research			x													
System documentation	x														x	
Threat assessment									x							
Vulnerability identification process		x														x

Table 4 Planning origin table

	NIST SP 800-161r1	Procurement guidelines for cybersecurity in hospitals	Secure ICT procurement in electronic communications	Österreichisches Informations-sicherheitshandbuch	Notional Supply Chain Risk Management Practices	Cloud Computing Kompass	Study on the need of Cybersecurity requirements for ICT	NPSA Protected Procurement	ENISA Procure Secure	OWASP SCVS	Guide on Cybersecurity Procurement Language in Task Order Requests	ENISA Security Guide for ICT Procurement	IT Grundschutz Kompendium	ISO/IEC 27036
Allocation of Resources	x													
Business Continuity Plan		x										x		
Contingency plan for termination of supplier relationship												x		
Definition of roles &												x		x

responsibilities														
Design governance structures	x							x						
Formalized development process	x													
Implementation plan	x			x									x	
Incident response plan		x							x		x	x	x	
Iterative improvement	x		x		x		x			x				
Open source policy										x				
Pentest after changes to the environment		x												
Policies	x		x	x						x		x	x	

Process for aquisition	x			x										
Strategic plan	x					x								
Usage of C-SCRM criteria	x													

Table 5 Requirements for products and services origin table

	NIST SP 800-161r1	Procurement guidelines for cybersecurity in hospitals	Secure ICT procurement in electronic communications	Österreichisches Informationssicherheitshandbuc	Indispensable baseline security requirements	SAFECode	Procurement guide for secure AI components	BSI TL-02103	Study on the need of Cybersecurity requirements for	NPSA Protected Procurement	ENISA Procure Secure	OWASP SCVS	ACSC Information Security Manual	Cybersecurity Procurement Language in Task Order	ENISA Security Guide for ICT Procurement	IT Grundschutz Kompendium	STAR Level 1: Security Questionnaire	OWASP ASVS	Beschaffung unter Berücksichtigung der IT	ISO/IEC 27036
Access to source code							x													
Asset protection					x										x					
Checklist of acquisition security requirements	x		x	x						x		x				x	x	x	x	
Establish logging on		x				x					x				x					

procured products																				
Gateways for legacy systems		x																		
Least privilege					x	x								x						x
List of security features														x						
Patching requirements		x						x			x									
Qualtiy management					x															
SBOM	x					x						x								
Security by design					x	x			x					x						
Service continuity					x						x				x					
Special treatment for customized components	x																			
Strong authentication					x				x											

Supply chain security					x							x	x						

Table 6 Requirements for suppliers origin table

	NIST SP 800-161r1	Procurement guidelines for cybersecurity in hospitals	Österreichisches Informations-sicherheitshandbuch	SAFECode	Procurement guide for secure AI components	BSI TL-02103	ENISA Procure Secure	OWASP SCVS	ENISA Security Guide for ICT Procurement	IT Grundschutz Kompendium	ISO/IEC 27036
Certification requirements		x				x					
Chain of custody				x				x			x
Developer screening	x										
Eligibility requirements		x	x								
Integrity protection											x
Maintenance		x	x		x		x			x	
Planning requirements		x	x								

Testing policy		x	x	x			x		x		

Table 7 Supplier relationship origin table

	NIST SP 800-161r1	Secure ICT procurement in electronic communications	Österreichisches Informations-sicherheitshandbuch	Notional Supply Chain Risk Management Practices	SAFECode	Procurement guide for secure AI components	BSI TL-02103	NPSA Protected Procurement	ENISA Procure Secure	OWASP SCVS	ACSC Information Security Manual	Guide on Cybersecurity Procurement Language in Task Order Requests	ENISA Security Guide for ICT Procurement	ISO/IEC 27036
Acceptance test			x		x									
Anonymous acquisition														x
Change management		x		x			x	x	x		x		x	
Contractual agreements	x		x			x		x	x		x		x	
Developer testing	x													
Limit access and exposure				x						x				

in the supply chain														
List of approved suppliers	x													
List of prohibited suppliers	x													

Table 8 Ongoing managerial tasks origin table

	NIST SP 800-161r1	ENISA Procurement guidelines for cybersecurity in hospitals	Secure ICT procurement in electronic communications	Österreichisches Informations-sicherheitshandbuch	Notional Supply Chain Risk Management Practices	Cloud Computing Kompass	Procurement guide for secure AI components	BSI TL-02103	Study on the need of Cybersecurity requirements for ICT products	ENISA Procure Secure	OWASP SCVS	ACSC Information Security Manual	Guide on Cybersecurity Procurement Language in Task Order Requests	ENISA Security Guide for ICT Procurement	IT Grundschutz Kompendium	ISO/IEC 27036
Awareness training	x				x			x	x				x	x	x	
Compliance management																x
Configuration management	x									x			x			
Interoperability management		x					x									
Risk management	x		x	x		x	x				x	x				

Threat management		x					x									
Vulnerability management		x							x	x					x	x

B. Interview summary SEC Consult

Eckdaten des Interviews

Das Interview wurde am 10.05.2023 von 9:30-10.15 via Microsoft Teams durchgeführt.

Interviewpartner

Thomas Kerbl ist seit ca. 20 Jahren als Security-Berater bei SEC Consult Unternehmensberatung GmbH tätig. In seiner Rolle als Principal Security Consultant und Teamleiter führt er nicht nur ein Expertenteam, sondern ist nach wie vor auch selbst in Kundenprojekten maßgeblich involviert. Seine aktuellen Schwerpunkte im Unternehmen sind die Bereiche "Sichere Software-Entwicklung / Software-Beschaffung" und "Security-Architektur".

Interview

Schinwald: Wie sieht Ihr idealer Lebenszyklus einer sicheren IT-Beschaffung aus?

Kerbl: Grundsätzlich ist im ersten Schritt zu unterscheiden, ob es sich bei der Beschaffung um ein “off the shelf” oder ein “customized” Produkt handelt. Der größte Unterschied hier ist, dass es bei bereits etablierten “off the shelf” Produkten schwieriger ist, Sicherheitsanforderungen nachträglich von Anbietern einzufordern. Lässt man jedoch eine maßgeschneiderte Lösung entwickeln, hat man als Kunde deutlich mehr Gestaltungsspielraum.

Eine Business Impact Analyse (BIA) lohnt sich, um im Vorfeld zu entscheiden, wie hoch das angestrebte Sicherheitsniveau sein muss. Handelt es sich um den lokalen Speiseplan im Intranet oder um eine Banken-Applikation? Um die verfügbaren Ressourcen für Applikationssicherheit bestmöglich einzusetzen, sollte deren Allokation auf den Ergebnissen der BIA basieren.

Bei kritischen Systemen kommt man an der Durchführung einer Bedrohungsmodellierung nicht vorbei. Im Rahmen einer solchen Bedrohungsmodellierung wird betrachtet, welche Daten ein System verarbeitet, wie diese im System transportiert und gespeichert werden, und welche Sicherheitsmechanismen bereits vorgesehen sind. Des Weiteren fließen Anforderungen aus relevanten Standards sowie rechtliche Rahmenbedingungen in die Analyse mit ein. Basierend auf den so identifizierten Bedrohungen können sinnvolle Architekturentscheidungen getroffen und – besonders wichtig im

Rahmen einer Beschaffung – Securit-Kriterien für die Produktauswahl definiert werden.

Hierbei ist es wichtig die Sicherheitsanforderungen mit anderen betriebswirtschaftlichen Anforderungen gleichzusetzen. Sicherheit darf kein sekundäres bzw. nachgelagertes Entscheidungskriterium sein, sondern muss von Beginn gleichwertig mit allen anderen Anforderungen betrachtet werden.

Wichtig ist es auch bei einer Beschaffung zu klären, wer die Kosten für den späteren Support trägt, sollten Security-Mängel aufgedeckt werden. Ohne eine vertragliche Grundlage kann es ansonsten zu Diskussionen kommen, welche Partei die Kosten für die Behebung einer Schwachstelle trägt. Aus Sicht des Kunden ist dies eine offensichtliche Mängelbehebung, während der Dienstleister einen Change Request argumentieren könnte. Definiert man bereits bei Auftragserteilung, wie mit solchen Fällen umzugehen ist, erspart man sich unnötige Streitigkeiten.

Weiters, ist ein Abnahmetest bei Erhalt des Produkts empfohlen, um sicher zu stellen, dass das Versprochene auch geliefert worden ist. Idealerweise erfolgt die Prüfung gegen die vorab definierten Sicherheitsanforderungen, es können aber auch etablierte Standards wie der OWASP ASVS als Prüfkatalog herangezogen werden.

Schinwald: Welcher Teil diese Lebenszyklus wird am häufigsten missachtet?

Kerbl: Für viele österreichische Unternehmen ist die Business Impact Analyse bereits ein fixer Bestandteil im Beschaffungsprozess. Es fehlt jedoch häufig das Verständnis für die daraus abzuleitenden Security Requirements.

Ein klassisches Beispiel ist die Forderungen von “Compliance with OWASP”, ohne näher zu spezifizieren, was damit konkret gemeint ist. OWASP ist eine Organisation, die zahlreiche Standards und Werkzeuge veröffentlicht. Eine zwar recht generische aber zumindest präzise Formulierung wäre: „Die Anwendung muss alle Anforderungen des OWASP ASVS Standards gemäß Level 2 erfüllen“.

In der Praxis trifft man jedoch nicht selten den zuvor geschilderten Fall an, dass lediglich „Compliance with OWASP“ gefordert wird. Auf die Rückfrage, was damit konkret gemeint ist, können weder Kunde noch Dienstleister eine zufriedenstellende Antwort geben. So kann Beschaffung von sicherheitskritischer Software nicht funktionieren!

Schinwald: Wann (wenn überhaupt) ist der Lebenszyklus abgeschlossen?

Kerbl: Auch wenn die Beschaffung formal mit dem Abnahmetest abgeschlossen ist, müssen Support-Prozesse und Vereinbarungen sicherstellen, dass die Anwendung bis zum Ende des Lebenszyklus ausreichend betreut wird. Wichtig ist ein Wartungsvertrag, in dem z.B. Themen wie Security Patches und Support im Falle eines Security-Incidents klar geregelt sind. Im besten Fall sind auch konkrete SLAs hinterlegt, um Zeitfenster für die Behebung kritischer Schwachstellen zu definieren.

Schinwald: Was sind Ihre präferierten Methoden, um für eine IT-Beschaffung Kontext zu schaffen?

Kerbl: Der Kontext wird im Wesentlichen durch die Bedrohungsanalyse geschaffen. Wichtig ist es hierbei sich nicht nur auf technische Aspekte zu fokussieren, sondern auch auf rechtliche Aspekte zu achten.

Schinwald: Gibt es Ihrer Meinung nach Prozesse, die selbst nach einer erfolgreichen Beschaffung weiterlaufen? Wenn, ja welche?

Kerbl: Beispiele für solche Prozesse wären z.B.:

- Maintenance und regelmäßige Update, die idealerweise via CI/CD automatisiert deployed werden
- Vulnerability Management, inkl. Updates von 3rd Party Komponenten im Falle von identifizierten Security Mängeln

Schinwald: Welche Aktivitäten sind für Sie bei der Planung einer sicheren Beschaffung wichtig?

Kerbl: Viele Unternehmen haben eine eigene Beschaffungsabteilung, die aber häufig nicht direkt mit den einzelnen Fachabteilungen spricht, um technische Details wir Security-Anforderungen zu konkretisieren. Das primäre Ziel der Beschaffungsabteilung ist es in der Regel, den bestmöglichen Preis für die Erfüllung von Mindestanforderungen zu erzielen. Security-Anforderungen können hierbei auf Kosten des Preises geopfert werden. Ein sehr teures Opfer, wenn man die Konsequenzen langfristig betrachtet.

Schinwald: Woran erkennt man, dass die Planung zur Genüge durchgeführt worden ist?

Kerbl: Ein reifer Beschaffungsprozess bindet die Security-Abteilung zwingen mit ein. Ist dies nicht der Fall und wird die Security Abteilung regelmäßig mit neu beschafften Systemen konfrontiert, bei denen Auswahl sie nicht involviert waren, besteht auf jeden Fall Handlungsbedarf. Bei Unternehmen, die zur kritischen Infrastruktur zählen, ist dies besonders wichtig.

Frage: Was sind für Sie die wichtigsten Sicherheitsanforderungen an Anbieter, die man als Beschaffer einfordern soll?

Die Sicherheitsanforderungen sollten sehr spezifisch auf das Umfeld des zu beschaffenden Systems zugeschnitten werden, aber folgende Anforderungen sind im Jahr 2023 aus meiner Sicht unverzichtbar:

Unverschlüsselte Protokolle sind nur in wirklich begründeten Ausnahmefällen akzeptabel. Der Overhead von Technologien wie TLS ist heutzutage vernachlässigbar. Eine fehlende Verschlüsselung bzw. der Einsatz als unsicher geltender Algorithmen ist ein absolutes no-go.

Automatisiertes Secrets Management, insbesondere im Cloud Umfeld.

Berücksichtigung von Risiken die aus dem Einsatz von 3rd party Komponenten entstehen sowie damit verbundene Supply Chain Angriffe.

Die Vermeidung der OWASP Top 10 ist ein absolutes Minimalkriterien. Besser wäre es zumindest die Einhaltung der Level 2 Anforderungen aus OWASP ASVS zu fordern.

Schinwald: Welche Zertifizierungen sollten Ihrer Meinung nach bei Lieferanten vorhanden sein?

Kerbl: Vor ein paar Jahren hätte ich diese Frage noch mit der ÖNORM A 7700 von Austrian Standards beantwortet. Leider kann man inzwischen Applikationen nicht mehr auf Basis dieser Norm zertifizieren lassen.

Alternativ kann jedoch OWASP ASVS hierfür herangezogen werden. OWASP bietet zwar selbst keine Zertifizierungen an, Security-Testern steht es jedoch frei, in eigenem Namen Compliance-Nachweise für ein spezifisches Level auszustellen.

Zertifizierungen sind häufig auch je nach Region unterschiedlich zu bewerten. In Deutschland hat das BSI einen hohen Stellenwert. Dies macht es für ein deutsches Unternehmen interessant, zu Anforderungen aus dem BSI Grundschutz wie z.B. Baustein APP.3.1 für Webanwendungen compliant zu sein.

Schinwald: Welche Frameworks können Sie zur sicheren IT-Beschaffung empfehlen?

Kerbl: Ich persönlich orientiere mich für sichere Entwicklung und Beschaffung an OWASP SAMM. Dieser Standard behandelt den gesamten Entwicklungsprozess von Software – die sichere Beschaffung ist ein Teil davon und kann in der Security Activity „Supplier Security“ gefunden werden.

Lässt man Software extern entwickeln, sollte man von seinem Dienstleister einen angemessenen Mindestreifegrad des Entwicklungsprozesses basierend auf OWASP SAMM einfordern.

Schinwald: Welche Trends erleben Sie im Bereich der sicheren Beschaffung?

Kerbl: Der Anteil von 3rd party Komponenten steigt stetig an. Das von diesen Komponenten ausgehende Risiko muss aktiv gemanaged werden.

Als positiven Trend nehme ich wahr, dass Testautomatisierung im Security Bereich immer mehr zum Standard wird. Security Scanner werden sofern möglich direkt in der CI/CD Pipeline integriert, wodurch bei jedem Build automatisch Dependencies überprüfen sowie der eigene Code auf Schwachstellen gescannt wird. Solche Automatismen können zwar eine tiefgehende manuelle Prüfung nicht ersetzen, bieten aber zumindest einen gewissen Grundschutz vor leicht zu identifizierenden Schwachstellen.

Im Bereich der kritischen Infrastruktur ist in den vergangenen Jahren deutlich mehr Awareness durch Regulierung geschaffen worden. Prüfstellen fordern aktiv Nachweise ein, die belegen, dass Software-Entwicklung und -Beschaffung mit der notwendigen Reife hinsichtlich Security durchgeführt werden.

Natürlich gibt es auch noch viele Unternehmen, die sichere Beschaffung noch gar nicht praktizieren. Viele Hersteller investieren zum Teil bewusst nicht in die Security ihrer Produkte, weil es schwierig ist, den “Return of Security Investment” objektiv darzustellen und einzupreisen. Entwicklung nach OWASP SAMM und vergleichbaren Standards führt zu deutlich höherer Software-Qualität, diese hat aber auch seinen Preis. Um kompetitive Preise am Markt anbieten zu können, verzichten daher manche Softwarehersteller auf wichtige Security Aktivitäten. Die Konsequenzen tragen dann die Kunden.

So negativ dies klingen mag – der Trend zeigt deutlich, dass Unternehmen immer mehr und mehr die Notwendigkeit von Security verstehen und daher auch bereit sind, für angemessene Qualität zu bezahlen. Langfristig rentiert sich dieses Investment und erspart viel Ärger.

Frage: Andere Themenbereiche der sicheren Beschaffung, die ich nicht abgedeckt habe?

Kerbl: Wenn ein Unternehmen die besprochenen Punkte durchgängig umsetzt, dann sind sie bereits in den Top 10% der Unternehmen in Österreich. Ich habe versucht ein Idealbild eines Beschaffungsprozesses aus Sicht der Security

darzustellen, bin mir aber bewusst, dass dies noch nicht in der Breite so gelebt wird.

Des Weiteren ist zu erwähnen, dass ich habe mich in unserem Interview stark auf den Softwarebereich fokussiert habe, aber viele der Punkte lassen sich auch sehr gut auf den Hardwarebereich übertragen.

C. Interview summary PWC

Eckdaten des Interviews

Interviewpartner

Erik Rusek ist seit 13 Jahren im Bereich der Cybersecurity tätig. Seit 4 Jahren ist er bei PWC für den Teilbereich “Information Security Strategy and Management” zuständig. Er beschäftigt sich außerdem mit regulativen und normativen Anforderungen und der Supply Chain.

Interview

Schinwald: Wie sieht Ihr idealer Lebenszyklus einer sicheren IT-Beschaffung aus?

Rusek: Das hängt stark davon ab, was man beschafft. Zum Beispiel muss man berücksichtigen, ob Hardware oder Software beschafft werden soll.

Idealerweise beginnt die Beschaffung mit dem Anforderungsmanagement. Es sollte eine Liste mit funktionalen und nicht funktionalen Anforderungen geben. Diese Anforderungen sollten sowohl intern als auch an den Lieferanten gestellt werden. Es ist wichtig hier schon Sicherheitskriterien in diese Anforderungen einfließen zu lassen.

Je nach Kritikalität sind auch gewisse Wirksamkeitsprüfungen zu empfehlen. Das können Dinge wie Pentests oder Checklisten sein. In der Regel möchte man auch die Anforderungen, die an den Lieferanten gestellt worden sind, überprüfen. Wichtig hier ist es, das nicht nur einmalig zu machen, sondern laufend. Besonders in kritischen Bereichen wie zum Beispiel dem Bankensektor.

Ein weiterer wichtiger Punkt ist das Management der Beziehung zum Lieferanten. Auch hier ist die Vorrausplanung essenziell. Themen wie das Offboarding des Lieferanten, Existenzszenarien oder spätere Nichtverfügbarkeit von Lieferanten sollten Beachtung finden.

Schinwald: Welcher Teil dieses Lebenszyklus ist für Sie der wichtigste?

Rusek: Wichtig ist es, bereits bei der Beschaffung Awareness zu schaffen. Security wird da oft stiefmütterlich bis gar nicht behandelt.

Schinwald: Welcher Teil diese Lebenszyklus wird am häufigsten missachtet?

Rusek: Häufig wird das Recht auf Audits im Vertrag vergessen. Außerdem ist nicht immer geklärt, wer für was verantwortlich ist.

Schinwald: Gibt es Ihrer Meinung nach Prozesse, die selbst nach einer erfolgreichen Beschaffung weiterlaufen? Wenn, ja welche?

Rusek: Auch hier ist es abhängig von dem, was gekauft wird. In dem Service Level Agreement sollten auch Monitoring und Informationssicherheitsüberprüfungen vereinbart werden. Wer das macht, ist weniger relevant, es nur wichtig, dass geklärt ist, wer verantwortlich ist und die Einhaltung überprüft.

Schinwald: Welche Aktivitäten sind für Sie bei der Planung einer sicheren Beschaffung wichtig?

Rusek: Die Rollen und Verantwortlichkeiten müssen geklärt sein. Die Inbetriebnahme sollte im Sinne der Verfügbarkeit der Fachabteilungen geplant werden. Auch auf die Zeit, die eine Schulung in Anspruch nimmt, sollte nicht vergessen werden.

Schinwald: Woran erkennt man, dass die Planung zur Genüge durchgeführt worden ist?

Rusek: Besitzt man eine unabhängige Checkliste, dann ist ausreichten geplant worden, wenn alles abgehakt worden ist.

Schinwald: Was sind für Sie die wichtigsten Sicherheitsanforderungen an Anbieter, die man als Beschaffer einfordern soll?

Rusek: Das hängt grundsätzlich davon ab, was Beschaffen werden soll. Zwei Anforderungen sollten aber bei allen Beschaffungen gestellt werden:

- • Mindeststandard an Security
- • Herstellerempfehlungen muss gefolgt werden

Schinwald: Welche Zertifizierungen sollten Ihrer Meinung nach bei Lieferanten vorhanden sein?

Rusek: Einerseits kann man Zertifizierungen wie ISO 27001 oder “CyberRisk Rating by KSV1870” einfordern. Andererseits sind auch branchenspezifische

Zertifizierungen zu empfehlen. Generell kann nicht immer sichergestellt, dass die Qualität der Zertifizierung passt.

Schinwald: Welche Frameworks können Sie zur sicheren IT-Beschaffung empfehlen?

Rusek: Es gibt keinen “golden Standard”, der nicht zertifizierbar ist. Als Beispiel kann man hier OWASP nennen. Jedoch ist es schwierig die Einhaltung nachzuweisen. Was bei österreichischen Firmen noch sehr beliebt ist NIS Compliance.

Schinwald: Welche Trends erleben Sie im Bereich der sicheren Beschaffung?

Rusek: Generell wird die Supply chain wird vermehrt für Cyberattacken verwendet. Es lässt sich auch ein Trend erkennen, bei dem immer mehr Fokus auf Sicherheit gelegt wird und Kontrollmaßnahmen härter werden.

Schinwald: Andere Themenbereiche der sicheren Beschaffung, die ich nicht abgedeckt habe?

Rusek: Es ist nicht zu vergessen, dass man als Lieferant auch Einfluss auf Kunden haben kann. Auch vertragsrechtliche Folgen darf man nicht übersehen.